ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.7, July 2007, pp.1799−1805
DOI: 10.1360/jos181799

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

椭圆曲线 Tate 对的压缩*

胡 磊+

(信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

Compression of Tate Pairings on Elliptic Curves

HU Lei+

(State Key Laboratory of Information Security (Graduate University, The Chinese Academy of Sciences), Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88256435, Fax: +86-10-88258713, E-mail: hu@is.ac.cn

Hu L. Compression of Tate pairings on elliptic curves. *Journal of Software*, 2007,18(7):1799−1805. http://www.jos.org.cn/1000-9825/18/1799.htm

Abstract: In this paper, utilizing maps between cyclic groups contained in a finite field, two efficient methods for compressing a Tate pairing defined on a supersingular elliptic curve with prime characteristic p and MOV degree 3 are presented. They compress a pairing value from a string of length of 6log$p$ bits to ones of 3log$p$ and 2log$p$ bits, respectively, and an implementation for both the compressed pairings makes use of the codes for the optimized algorithm of the original pairing and no new code is needed. Both the compressed pairings achieve the speed of the original implementation.

Key words: Tate pairing; elliptic curve; compressed Tate pairing; algebraic torus; identity based cryptosystem

摘 要: 利用有限域包含的循环群之间的映射,给出了特征为素数 p,MOV 次数为 3 的超奇异椭圆曲线上的一类 Tate 对的两种有效压缩方法,它们分别将 Tate 对的值从 6log$p$ 比特长的串压缩到 3log$p$ 和 2log$p$ 比特长.两种压缩方法的实现均使用原有 Tate 对的优化算法的代码,不需要针对压缩对编写新的实现代码,而且两种压缩对的实现均保持原有 Tate 对的实现速度.

关键词: Tate 对;椭圆曲线;压缩 Tate 对;代数环面;基于身份的密码系统
中图法分类号: TP309 文献标识码: A

1 Introduction

Recently, Tate pairings over elliptic curves become a hotspot in the field of cryptographic research. Tate pairing is an efficiently computable bilinear map associated with elliptic curves, based on a pairing related, reasonably presumed computationally hard problem, namely the bilinear Diffie-Hellman problem, many identity based cryptographic schemes were proposed (see Refs.[1−7] and references therein).

Let E be an elliptic curve defined over a finite field $GF(q)$, l be a prime factor of $\#E(GF(q))$. Let k be the

* Supported by the National Natural Science Foundation of China under Grant Nos.90104034, 60373041 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2002AA141020 (国家高技术研究发展计划(863))

Received 2004-07-06; Accepted 2006-03-09

minimal integer such that all l-torsion points of $E(\overline{GF(q)})$ are contained in $E(GF(q^k))$, where $\overline{GF(q)}$ is the algebraic closure of $GF(q)$. Originally, a Tate paring is defined over the group of all l-torsion points of $E(GF(q^k))$ and the values of the pairing are elements of the quotient group $GF(q^k)^*/(GF(q^k)^*)^l$. Let $E(GF(q^k))[l]$ and $E(GF(q))[l]$ denote the group of all l-torsion points of $E(GF(q^k))$ and $E(GF(q))$, respectively. By using a distortion map defined on E, one can define a modified Tate pairing on $E(GF(q))[l]$ instead of on $E(GF(q^k))[l]$, and this improves the efficiency of the setup of cryptosystems established over the pairing. To eliminate the ambiquity caused by the non-uniqueness of coset representative of elements of $GF(q^k)^*/(GF(q^k)^*)^l$, a $(q^k-1)/l$-powering to the pairing values is usually operated, and the pairing values are then defined as elements of $(GF(q^k)^*)^{(q^k-1)/l}$. In general, there needs a string of length of $k\log q$ bits to represent one element in $GF(q^k)^*$ and in its subset $(GF(q^k)^*)^{(q^k-1)/l}$. Strings of the same length are needed for $GF(q^k)^*/(GF(q^k)^*)^l$.

However, the pairing values form a subgroup of $GF(q^k)^*$ of order l. Information-theoretically speaking, the values should be represented in strings of length of $\log l$ bits, or in strings of at most $\log q+1$ bits, since $l\le\#E(GF(q))\le 2q$. The problem is how to find an efficient method which computes a lossless representation for each pairing value.

Any method of representation in less than $k\log q$ bits is meaning. This problem is data compression and it is useful in many cryptographic applications. For example, in some pairing based cryptosystems (see Refs.[1−7]), the values of the Tate pairing are part of the system parameter (f.g., the public key of a user, the ciphertext, or the transposed message, etc.) a data compression of pairing values gives a saving of storage or communication bandwidth.

In this paper, we propose two lossless data compression methods for the Tate pairing whose efficient implementation was studied in Ref.[8]. The implementation of the pairing in Ref.[8] is primarily designed to re-use low-level codes developed in usual implementation of elliptic curve cryptosystems over $GF(p)$. It is a first study of implementation of Tate pairings defined over supersingular elliptic curves of MOV degree 3 and has very fast implementation speed. See Ref.[8] for its details and see also Section 2. The first compression method we proposed here compresses the pairing values from strings of length of $6\log p$ bits to ones of $3\log p$ bits, whilst it completely preserves the implementation speed of the optimized algorithm studied in Ref.[8]. The second compresses the pairing values to strings of length of $2\log p$ bits and is an optimized compression theoretically (see Section 4), but its implementation needs very few extra computation in addition to the optimized algorithm in Ref.[8]. No new code is needed for the implementation of both new pairings. Similar results on compression of pairing value are given in Refs.[9,10]. However, these compression methods are primarily designed for Tate pairings defined over supersingular elliptic curves of characteristic 3 and MOV degree 6, and are associated with the specific pairing evaluation algorithm of Duursma and Lee[11]. They are not applicable to our case and are very different with our analysis.

2 Elliptic Curve and Original Tate Pairing

Let p be a prime congruent to 11 modulo 12. We assume p is large, for instance, p is of length of 192 bits as in the implementation studied in Ref.[8]. In Ref.[8], a method is presented to find a small integer u such that $(x^3-u)^2+1$ is an irreducible polynomial over $GF(p)$. Let β be a root of $(x^3-u)^2+1$ in $GF(p^6)$. Then $\rho=\beta^3$ belongs to the subfield $GF(p^2)$ and it is not a cube in the subfield[8]. The fields $GF(p^6)$ and $GF(p^2)$ are respectively represented as

$$GF(p^6)=\{a_0+a_1\beta+\ldots+a_5\beta^5:a_0,\ldots,a_5\in GF(p)\}$$

and

$$GF(p^2)=\{a_0+a_3\beta^3:a_0,a_3\in GF(p)\}.$$

The arithmetic of $GF(p^6)$ and $GF(p^2)$ are analyzed in Ref.[8].

Let E be an elliptic curve defined over $GF(p^2)$ by the equation

$$y^2=x^3+\rho^2.$$

E is supersingular, and the order of $E(GF(p^2))$ is p^2-p+1.

Let l be a prime factor of p^2-p+1 not dividing p^2-1. Assume l is sufficiently large, e.g., the length of l is more than 160 bits as specified in Ref.[8]. The MOV degree of E associated with l is 3, i.e., $E(\overline{GF(p^2)})[l]\subset E(GF(p^6))$ but $E(\overline{GF(p^2)})[l]\not\subset E(GF(p^{2i}))$ for i=1 or 2. Define a distortion map on $E/GF(p^2)$ as follows:

$$\begin{cases}\Phi: E/GF(p^2)\to E/GF(p^6)\\ (x,y)\mapsto(a\beta x^p, by^p)\end{cases},$$

where $a=\rho^{-(2p-1)/3}\in GF(p^2)$ and $b=\rho^{-(p-1)}\in GF(p^2)$. Then the Tate pairing of order l, e_l, is defined to map a pair (P,Q) of points of $E(GF(p^2))[l]$ to

$$e_l(P,Q)=f_P(\Phi(Q))^{(p^6-1)/l}\in GF(p^6),$$

where f_P is a rational function defined on E with divisor $(f_P)=l(P)-l(O)$.

Miller's algorithm evaluates $f_p(\Phi(Q))$ iteratively. For the details of the algorithm, see the pseudo-code given in Ref.[8] or the appendix in Ref.[12]. Set $f=f_p(\Phi(Q))$.

Using the linearity property of the p-powering over a field of characteristic p, an algorithmic technique is presented in Ref.[8] to speed up the calculation of $f^{(p^6-1)/l}$, which is a time-consuming powering over the extension field $GF(p^6)$. The technique will be also used for the first compressed Tate pairing proposed in the next section, and we present it here as Fig.1. Here k_1 and k_0 are defined by $(p^2-p+1)/l=k_1p+k_0$ and $0\le k_0,k_1<p$.

1. Compute $g\leftarrow f^{k_1}$ and $f\leftarrow f^{k_0}$
2. Compute $g\leftarrow g^p$ and $f\leftarrow gf$
3. Compute $g\leftarrow f^p$ and $f\leftarrow gf$
4. Compute $g\leftarrow((f^p)^p)^p$ and $f\leftarrow f^{-1}$
5. Compute $f\leftarrow gf$ and return (f)

Fig.1 Fast $(p^6-1)/l$-powering

It is shown that a p-powering calculation needs at most eight $GF(p)$-multiplications and it can be regarded as free comparing to a full powering[8]. In a concrete implementation in Ref.[8], l is chosen to be of near size as p, and so, k_1 is usually small (may be zero) and the calculation of f^{k_0} is the dominant step in the algorithm. The technique has an efficiency improvement of four to five times comparing to a direct method.

3 A Compressed Tate Pairing

Let G be a cyclic group of order n, and m be a factor of n. Set $G^m=\{a^m: a\in G\}$. Then G^m is a cyclic subgroup of order n/m. Let l be a factor of m. Define a map π between two quotient groups G/G^l and $G^{m/l}/G^m$ by mapping $aG^l\in G/G^l$ to $a^{m/l}G^m\in G^{m/l}/G^m$.

Lemma 1. The map is well-defined and is an isomorphism of groups.

Fix $G=GF(p^6)^*$, $n=p^6-1$, and l, and denote π by π_m. The Tate pairing mentioned in the previous section is $e_l(P,Q)=\pi_{p^6-1}(fG^l)$. We below fix $m=p^3+1$ and consider to define a new Tate pairing relative to $\pi_m(fG^l)$.

Obviously, we have $G^m=GF(p^3)^*$, because both sides are cyclic subgroups of $GF(p^6)^*$ of order p^3-1. Let $\{\gamma_1,\gamma_2\}$ be a basis of $GF(p^6)$ over $GF(p^3)$. Define a map Γ from G/G^m to $GF(p^3)\cup\{\infty\}$ as follows: for

$$c=c_1\gamma_1+c_2\gamma_2, c_1,c_2\in GF(p^3),$$

define $\Gamma(cG^m)=c_1/c_2$, where ∞ is a special notation and we assume that $c_1/0=\infty$.

Lemma 2. The map Γ is well-defined and is a bijection.

Let $\{\delta_1,\delta_2\}$ be the dual basis of $\{\gamma_1,\gamma_2\}$, i.e., $\mathrm{Tr}(\delta_i\gamma_i)=1$ and $\mathrm{Tr}(\delta_i\gamma_j)=0$ for $1\le i\ne j\le 2$, where Tr is the trace map of $GF(p^6)$ over $GF(p^3)$. Then

$$c_i = \mathrm{Tr}(c\delta_i) = c\delta_i + (c\delta_i)^{p^3}.$$

Take δ_1=1 and δ_2=β. Then

$$\Gamma(cG^m) = \frac{c + c^{p^3}}{c\beta + (c\beta)^{p^3}}$$

and its calculation needs six p-powerings and one $GF(p^6)$-inversion (regarding a multiplication by β as free).

Write each element of $GF(p^6)$ as a six-dimensional vector over $GF(p)$, whose components are the six coefficients of the polynomial expression in β of the element. Since $GF(p^3)$ is a three-dimensional $GF(p)$-linear subspace of $GF(p^6)$, there exist three fixed component positions such that different elements of $GF(p^3)$ have different three-dimensional sub-vectors at these positions.

Now we define the final pairing value of a compressed Tate pairing, $\overline{e_l}(P,Q)$, as the three-dimensional sub-vector of

$$\Gamma(\pi_m(fG^l)) = \Gamma(f^{(p^3+1)/l}G^m).$$

It is the special notation ∞ if $f^{(p^3+1)/l}\beta + (f^{(p^3+1)/l}\beta)^{p^3} = 0$, and is a three-dimensional vector over $GF(p)$ otherwise.

1. Compute $g \leftarrow f^{k_1}$ and $f \leftarrow f^{k_0}$
2. Compute $g \leftarrow g^p$ and $f \leftarrow gf$
3. Compute $g \leftarrow f^p$, $f \leftarrow gf$ and return (f)

Fig.2 Fast (p^3+1)/l-powering

By Lemma 1 and Lemma 2, we have

Proposition 1. $\overline{e_l}$ is a lossless compression of the pairing e_l, i.e., if $\overline{e_l}(P_1,Q_1) = \overline{e_l}(P_2,Q_2)$ for $P_1,Q_1,P_2,Q_2 \in E(GF(p^2))[l]$, then $e_l(P_1,Q_1)=e_l(P_2,Q_2)$.

The calculation of $\Gamma(f^{(p^3+1)/l}G^m)$ includes the calculation of the (p^3+1)/l-powering, namely $c = f^{(p^3+1)/l}$, and that of $(c + c^{p^3})/(c\beta + (c\beta)^{p^3})$. The former is similar to the (p^6−1)/l-powering and is shown in Fig.2. Comparing it with the (p^6−1)/l-powering calculation shown in Fig.1, it is easy to know that $e_l(P,Q)$ and $\overline{e_l}(P,Q)$ have almost the same computational complexity. All calculations for $\Gamma(f^{(p^3+1)/l}G^m)$, including that for $f^{(p^3+1)/l}$ and that for $(c + c^{p^3})/(c\beta + (c\beta)^{p^3})$, can be operated according to arithmetic of elements of $GF(p^6)$. So, no code for arithmetic of $GF(p^3)$ is needed, although this subfield is involved in the definition of the compressed Tate pairing. The implementation of both (compressed and non-compressed) Tate pairings can make use of the same implementation codes.

4 Another Optimal Compressed Tate Pairing

In this section we give another compression method. It directly compresses the original pairing value defined in Section 2 from $f^{(p^6-1)/l}$, does not compresses the pairing value from $f^{(p^3+1)/l}$. The compressed pairing value composes of two $GF(p)$-elements.

Let $h = f^{(p^6-1)/l}$. Since l divides p^3+1 and p^4+p^2+1, we have

$$h^{p^3+1} = 1, \quad h^{p^4+p^2+1} = 1.$$

Very recently, a new concept, algebraic torus, is introduced into cryptography to generalize public key schemes with short keys such as XTR and GH cryptosystems[13] and to study compression of pairing[10]. We utilize the idea of this concept and the result in Ref.[10] to develop a new pairing in this section.

Let $\alpha=\beta^3-u$. Then α is an element in $GF(p^2)$ and satisfies $\alpha^2=-1$ and $\alpha^p=-\alpha$. Let

$$h = \frac{a+\alpha}{a-\alpha}.$$

From $h^{p^3+1} = 1$, i.e.,

$$\frac{a^{p^3}-\alpha}{a^{p^3}+\alpha} \cdot \frac{a+\alpha}{a-\alpha} = 1,$$

we have $a^{p^3}=a$ and $a\in GF(p^3)$. When a ranges over $GF(p^3)$, $\frac{a+\alpha}{a-\alpha}$ ranges over all elements h in $GF(p^6)\backslash\{1\}$ that satisfy $h^{p^3+1}=1$. Thus we have

Lemma 3. The map Δ that maps 1 to ∞ and maps non-identity element h to $a=\alpha\frac{h+1}{h-1}$ is a bijection from G^{p^3-1} (the subgroup of $GF(p^6)^*$ of order p^3+1) to $GF(p^3)\cup\{\infty\}$.

Further, from $h^{p^4+p^2+1}=1$ and $a^{p^3}=a$, we have

$$\frac{a^p+\alpha}{a^p-\alpha}\cdot\frac{a^{p^2}+\alpha}{a^{p^2}-\alpha}\cdot\frac{a+\alpha}{a-\alpha}=1,$$

and hence have

$$a^{p+1}+a^{p^2+1}+a^{p^2+p}=1,$$

and $\mathrm{tr}(a^{p+1})=1$, where tr is the trace map of $GF(p^3)$ over $GF(p)$.

The above analysis is discussed in Ref.[10] for compression of a Tate pairing defined over a class of elliptic curves of characteristic 3 and of MOV degree 6. Due to the property of characteristic 3, there always exists a special irreducible polynomial over $GF(3^{2n})$ which defines $GF(3^{6n})$, and this deduces a direct compression for the values of a ($\in GF(3^{2n})$ in Ref.[10]). However, it is not the case for our study here and we need a new compression for $a\in GF(p^3)$.

By a well known result on normal base of finite field (see Theorem 1.4.4 cited in Page 10 in Ref.[14]), there exists a self-dual normal base of $GF(p^3)$ over $GF(p)$. By applying Theorem 5.4.4 of Ref.[14], a self-dual normal base can be constructed and it composes of the three roots of the irreducible polynomial of the form $x^3-x^2+(\tau+1)^2/(27\tau)$, where τ is an element of $GF(p^2)$ of order $p+1$ (it must satisfy $(\tau+1)^2/\tau\in GF(p)$). These three roots can be computed according to the Berlekamp algorithm for any finite field (here for $GF(p^6)$) (see Page 133 in Ref.[15]).

Let γ be a root in $GF(p^3)$ of $x^3-x^2+(\tau+1)^2/(27\tau)$. Let

$$a=a_1\gamma+a_2\gamma^p+a_3\gamma^{p^3},\ a_1,a_2,a_3\in GF(p).$$

Since $\mathrm{tr}(a^{p+1})=1$, we have

$$(a_1a_2+a_1a_3+a_2a_3)\mathrm{tr}(\gamma^2)=1.$$

So a_3 is uniquely determined by a_1 and a_2. a_1 and a_2 can be computed by

$$a_1=\mathrm{tr}(a\gamma),a_2=\mathrm{tr}(a\gamma^p).$$

By the bilinearity and non-degeneracy of the Tate pairing, and since e_l is defined over a group of prime order, we know that $e_l(P,Q)=1$ if and only if P or Q is the point at infinite O. Define $\overline{e_l'}(P,O)=\overline{e_l'}(O,Q)=\infty$ and

$$\overline{e_l'}(P,Q)=(\mathrm{tr}[\Delta(e_l(P,Q))\gamma],\mathrm{tr}[\Delta(e_l(P,Q))\gamma^p])$$

for $P,Q\neq O$, where Δ is defined in Lemma 3. By Lemma 3 and the above discussion, we have

Proposition 2. $\overline{e_l'}$ is a lossless compression of the pairing e_l.

Remark 1. Any compressed representation of e_l must have a length of $\log l$ bits since $e_l(P,Q)$ may take each of the l values. Since l divides p^2-p+1, we know that for some p, l may be of size of near p^2, and for such p and l, a compressed representation of e_l must have a length of $2\log p$ bits. In this sense, $\overline{e_l'}$ is an optimal compression of e_l.

In the implementation of $\overline{e_l'}$, $a=\Delta(e_l(P,Q))$, γ, and γ^p are represented as polynomials in β, and $a\gamma$ and $a\gamma^p$ are calculated according to $GF(p^6)$-multiplication.

Let w_i be the constant term of $\beta^i+\beta^{ip}+\beta^{ip^2}$ as a polynomial in β of degree less than 6, $1\leq i\leq 5$. (Here we note that in general $\beta^i+\beta^{ip}+\beta^{ip^2}$ is not an element of $GF(p)$ since $\beta\notin GF(p^3)$.) Let

$$a\gamma=b_0+b_1\beta+\ldots+b_5\beta^5, a\gamma^p=c_0+c_1\beta+\ldots+c_5\beta^5,$$

where $b_i,c_i\in GF(p)$. Then

$$a_1=3b_0+b_1w_1+\ldots+b_5w_5, a_2=3c_0+c_1w_1+\ldots+c_5w_5.$$

Remark 2. $\gamma,\gamma^6\in GF(p^6)$ and $w_1,\ldots,w_5\in GF(p)$ can be calculated as part of the system parameter.

The algorithm to compute $\overline{e_l'}(P,Q)$ for $P,Q\neq O$ is listed in Fig.3. From this figure, we conclude that the computation of $\overline{e_l'}(P,Q)$ needs, in addition to that for $e_l(P,Q)$, one $GF(p^6)$-inversion, two $GF(p^6)$-multiplications and ten $GF(p)$-multiplications (neglecting a multiplication by α). As for $\overline{e_l}$, the implementation of $\overline{e_l'}$ makes use of the same implementation codes for e_l.

1. Compute $h\leftarrow e_l(P,Q)$ and $a\leftarrow\alpha(h+1)/(h-1)$
2. Compute $b_0,b_1,\ldots,b_5\in GF(p)$ with $a\gamma=b_0+b_1\beta+\ldots+b_5\beta^5$
3. Compute $c_0,c_1,\ldots,c_5\in GF(p)$ with $a\gamma^p=c_0+c_1\beta+\ldots+c_5\beta^5$
4. Compute $a_1=3b_0+b_1w_1+\ldots+b_5w_5, a_2=3c_0+c_1w_1+\ldots+c_5w_5$
5. Return (a_1,a_2)

Fig.3 Computing $\overline{e_l'}(P,Q)$ for $P,Q\neq O$

5 Conclusions

Compression of values of Tate pairings is useful for the application of identity based cryptography. We present two methods to efficiently compress values of the Tate pairing that is defined on the supersingular elliptic curves with general prime characteristic p and MOV degree 3 and is first studied in Ref.[8], one has compression rate of 1/2 and the other is theoretically optimal and has compression rate of 1/3. The proposed methods also achieve the original design goal of the study in Ref.[8] that re-uses low-level codes developed in usual elliptic curve cryptosystem implementation over $GF(p)$, and need no extra new code for their implementation. In addition, their implementation speed is fast as that for the original pairing.

References:

[1] Joux A. The weil and tate pairings as building blocks for public key cryptosystems. In: Fieker C, Kohel DR, eds. Algorithm Number Theory Symposium-ANTS-V. Berlin, Heidelberg: Springer-Verlag, 2002. 20−32.

[2] Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme. In: Biham E, ed. Advances in Cryptology-EUROCRPYT 2003. Berlin, Heidelberg: Springer-Verlag, 2003. 255−271.

[3] Bohen D, Boyen X. Efficient selective-id secure identity based encryption without random oracles. In: Cachin C, Camenisch J, eds. Advances in Cryptology-EUROCRYPT 2004. Berlin: Springer-Verlag, 2004. 223−238.

[4] Boneh D, Mironov I, Shoup V. A secure signature scheme from Biliear maps. In: Joye M, ed. The Cryptographers' Track at the RSA Conf.-CT-RSA 2003. Berlin, Heidelberg: Springer-Verlag, 2001. 98−110.

[5] Steinfeld R, Bull L, Wang H, Pieprzyk J. Universal designated-verifier signatures. In: Laih CS, ed. Advances in Cryptology-ASIACRYPT 2003. Berlin: Springer-Verlag, 2003. 523−542.

[6] Barreto PSLM, Kim H, Lynn B, Scott M. Efficient algorithms for pairing based cryptosystems. In: Yung M, ed. Advance in Cryptology-Crypto 2002. Berlin, Heidelberg: Springer-Verlag, 2002. 354−368.

[7] Galbraith SD, Harrison K, Soldera D. Implementing the tate pairing. In: Fieker C, Kohel DR, ed. Algorithm Number Theory Symposium-ANTS-V. Berlin, Heidelberg: Springer-Verlag, 2002. 324−337.

[8] Hu L, Dong J, Pei D. An implementation of cryptosystems Basedon tate pairing. Journal of Computer Science and Technology, 2005,20(2):264−269.

[9] Scott M, Barreto P. Compressed pairings. In: Franklin M, ed. Advances in Cryptology-CRYPTO 2004. Berlin, Heidelberg: Springer-Verlag, 2004. 140−156. http://ePrint.iacr.org/2004/032.pdf (Cryptology ePrint Archive, Report 2004/032).

[10] Granger R, Page D, Stam M. On small characteristic algebraic Tori in pairing-based cryptography. http://ePrint.iacr.org/2004/132.pdf (Cryptology ePrint Archive, Report 2004/132).

[11] Duursma I, Lee H. Tate pairing implementations for tripartite key agreement. In: Laih CS, ed. Advances in Cryptology-ASIACRYPT 2003. Berlin: Springer-Verlag, 2003. 111−123.

[12] Boneh D, Franklin M. Identity based encryption from the weil pairing. In: Kilian J, ed. Advance in Cryptology-Crypto 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 213−229.

[13] Rubin K, Silverberg A. Algebraic Tori in cryptography. In: High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Institute Communications Series, American Mathematical Society. 2003. http://www.math.uci.edu/~asilverb/bibliography/tori.pdf

[14] Gao S. Normal bases over finite fields [Ph.D. Thesis]. Waterloo: University of Waterloo, 1993. http://www.math.clemson.edu/~sgao/

[15] Cohen H. A Course in Computational Algebraic Number Theory. Berlin, Heidelberg: Springer-Verlag. 1993.

HU Lei was born in 1967. He is a professor at the Graduate University, the Chinese Academy of Sciences. His current research areas are cryptography and information security.

****

第 9 届国际信息与通信安全会议(ICICS 2007)

征 稿 通 知

2007 年 12 月 12－15 日 中国 河南 郑州

http://www.ICICS2007.org.cn/

2007 年国际信息与通信安全会议是(ICICS 2007)第 9 届 ICICS 系列会议。与前 8 届 ICICS 系列会议相同，ICICS 2007 将为国内外信息安全学者与专家齐聚一堂，提供探讨国际信息安全前沿技术的难得机会。作为国际公认的第一流国际会议，ICICS 2007 将进一步促进国内外的学术交流，促进我国信息安全学科的发展。本次学术会议将由中国科学院软件研究所和北京大学软件与微电子学院主办，由中安科技集团承办，并得到国家自然基金委员会和河南省人民政府信息化办公室的大力支持。

会议欢迎来自全世界所有未发表过和未投递过的原始论文，内容包括，但不限于以下内容：访问控制；计算机病毒与蠕虫对抗；认证与授权；应用密码学；生物安全；数据与系统安全；数据库安全；分布式系统安全；电子商务安全；欺骗控制；网格安全；信息隐藏与水印；知识版权保护；入侵检测；密钥管理与密钥恢复；基于语言的安全性；操作系统安全；网络安全；风险评估与安全认证；无线安全；安全模型；安全协议；可信计算。

投稿须知：作者提交的论文，必须是未经发表或未并行地提交给其他学术会议或学报的原始论文。所有提交的论文都必须是匿名的(没有作者名字，单位名称，致谢或其他明显透露身份的内容)。论文必须用英文，并以 PDF 或 PS 格式提交。排版字号为 11pt，且论文不能超过 12 页(A4 纸)。所有提交论文必须在无附录的情形下是可理解的。如果提交论文未遵守上述要求，论文作者将自行承担论文未通过形式审查而拒绝接受论文的风险。审稿将由 3 位程序委员匿名评审，评审结果为：以论文形式接受；以短文形式接受；拒绝接受。

ICICS2007 会议论文集将由德国 Springer 出版社作为 LNCS 系列出版，可在会议期间获取。凡接受论文的作者中，至少有 1 位必须参加会议，并在会议上报告论文成果。

投稿截止时间：2007 年 8 月 1 日

通知接受时间：2007 年 9 月 17 日

发表稿提交截止时间：2007 年 10 月 1 日