The Well-Tempered Pairing

Paulo S. L. M. Barreto
University of São Paulo

Outline

- Algorithms for pairing computation (variants of Miller's algorithm).
- New derivation and generalization of the Duursma-Lee algorithm.
- Effects of pairing choice upon protocols:
  - Processing speed vs. storage requirements.
  - Cryptographic properties.

Acknowledgements

- This talk contains several results of my joint work with:
  - Steven Galbraith
  - Noel McCullagh
  - Mike Scott

  who gave their kind permission to quote those results.
- Harpsichord image courtesy of Bob Hearn.

Preliminaries

- Let E be an elliptic curve over $\mathbf{F}_q$ with $q = p^m$ containing a subgroup of prime order r with even embedding degree $k = 2d$.
- Let $P \in E(\mathbf{F}_q)$. Define $f_{n,P}$ to be a function with divisor $(f_{n,P}) = n(P) - (nP) - (n-1)(O)$.
- The Tate pairing of order r is the bilinear map $\langle , \rangle_r : E(\mathbf{F}_q)[r] \times E(\mathbf{F}_{q^k})/rE(\mathbf{F}_{q^k}) \rightarrow \mathbf{F}^*_{q^k} / (\mathbf{F}^*_{q^k})^r$ given by $\langle P,Q \rangle_r = f_{r,P}(Q)$ (N.B. defined only up to r-th powers).

Distortion maps

- A distortion map $\psi : E(\mathbf{F}_{q^k}) \rightarrow E(\mathbf{F}_{q^k})$ is a non-$\mathbf{F}_q$-rational endomorphism, i.e. $\psi(P) \notin \langle P \rangle$.
- In practice the first argument is restricted to $E(\mathbf{F}_q)$.
  - $E_{2,b}$: $y^2 + y = x^3 + x + b$ over $\mathbf{F}_2$.
    $\psi(x, y) = (x + s + 1, y + sx + t)$
    where $s \in \mathbf{F}_{2^2}$ and $t \in \mathbf{F}_{2^4}$ satisfy
    $s^2 = s + 1$ and $t^2 = t + s$.
  - $E_{3,b}$: $y^2 = x^3 - x + b$ over $\mathbf{F}_3$.
    $\psi(x, y) = (-x + \rho, \sigma y)$
    where $\sigma \in \mathbf{F}_{3^2}$ and $\rho \in \mathbf{F}_{3^3}$ satisfy
    $\sigma^2 = -1$ and $\rho^2 = \rho + b$.

Tate pairing(s)

- The *reduced* Tate pairing is the bilinear map $e: E(\mathbf{F}_q)[r] \times E(\mathbf{F}_{q^k}) \to \mathbf{F}^*_{q^k}$ given by $e(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}$.
- The *modified* Tate pairing is the bilinear map $\hat{e}: E(\mathbf{F}_q)[r] \times E(\mathbf{F}_q)[r] \to \mathbf{F}^*_{q^k}$ given by $\hat{e}(P,Q) = f_{r,P}(\psi(Q))^{(q^k-1)/r}$.
- Let N be a multiple of r that divides $q^k - 1$. The reduced and modified pairings can be equivalently computed using order N: $f_{r,P}(.)^{(q^k-1)/r} = f_{N,P}(.)^{(q^k-1)/N}$.

Miller's algorithm

- Miller showed how to compute $f_{n,\mathrm{P}}$ iteratively, using the divisors of the lines drawn by the secant-and-tangent addition rule.
- Improved algorithms (Barreto et al., Galbraith et al.) eliminate redundancies in Miller's algorithm – factors from subfields are wiped out by the final powering and can be omitted.
- ... but it is possible to simplify the algorithms even more.

Towards a simplified algorithm

- For supersingular curves, compute the pairing of order $N = q^d + 1$, i.e. $\hat{e}(P,Q) = f_{q^d+1,P}(\psi(Q))^{q^d-1}$. Note the simple final powering.
- Claim: since $q^d P = -P$, there is a function v_P with divisor $(v_P) = (P) + (q^d P) - 2(O)$, hence $f_{q^d+1,P} = f_{q^d,P} \cdot v_P$.

Towards a simplified algorithm

- Proof: v_P is obviously the vertical line through P and –P. From the definition of $f_{n,P}$ we have $(f_{q^d+1,P}) = (q^d + 1)(P) - ((q^d + 1)P) - (q^d)(O) = q^d(P) - (q^dP) - (q^d - 1)(O) + (P) + (q^dP) - 2(O) = (f_{q^d,P}) + (v_P)$ as expected.
- But $v_P(\psi(Q)) \in \mathbf{F}_{q^d}$ is wiped out by the powering to $q^k - 1$, so we can write simply $\hat{e}(P,Q) = f_{q^d,P}(\psi(Q))^{qd-1}$.

Towards a simplified algorithm

- Claim: in characteristic *p* we can write a *p*-ary iterative algorithm to compute ê(P, Q):

$$f_{q^d,P}(\psi(Q)) = \prod_{i=0}^{dm-1} f_{p,p^i P}^{\,p^{dm-1-i}}(\psi(Q))$$

Towards a simplified algorithm

- Proof: recall that, by definition, $(f_{n,\mathrm{V}}) = n(\mathrm{V}) - (n\mathrm{V}) - (n-1)(\mathrm{O})$. Hence:
- $(f_{p^{i+1},\mathrm{V}}) = p^{i+1}(\mathrm{V}) - (p^{i+1}\mathrm{V}) - (p^{i+1}-1)(\mathrm{O})$

$$= p[p^{i}(\mathrm{V}) - (p^{i}\mathrm{V}) - (p^{i}-1)(\mathrm{O})] + p(p^{i}\mathrm{V}) - (p \cdot p^{i}\mathrm{V}) - (p-1)(\mathrm{O})$$

$$= p(f_{p^{i},\mathrm{V}}) + (f_{p,p^{i}\mathrm{V}}).$$

- Thus $f_{p^{i+1},\mathrm{V}} = (f_{p^{i},\mathrm{V}})^{p} \cdot f_{p,p^{i}\mathrm{V}}$.

recurrence on i

compute piV *on the fly*

Towards a simplified algorithm

- We now define the η *pairing* as:

$$\eta(P,Q) = \prod_{i=0}^{m-1} f_{p,p^i P}^{p^{m-1-i}}(\psi(Q))$$

- Theorem: the η pairing is bilinear and non-degenerate for certain choices of ψ. Thus, it satisfies the property:
- $f_{q^d,P}(\psi(Q)) = \eta(P,Q)^{p^{m(d-1)}} \cdot \eta(p^m P,Q)^{p^{m(d-2)}} \cdot \ldots \cdot$

$$\eta(p^{m(d-2)}P,Q)^{p^m} \cdot \eta(p^{m(d-1)}P,Q)$$

$$= \eta(P,Q)^{dq^{d-1}}.$$

Towards a simplified algorithm

- The powering to q^{d-1} can be easily avoided by including the Frobenius action as part of the distortion map without any substantial extra cost.
- The powering to d can also be avoided in the special case $d = p$, but this involves slightly changing the function $f_{p,\mathrm{P}}$ as well.

Towards a simplified algorithm

- The $\eta(P,Q)^{q^d-1}$ pairing itself (without the powering to dq^{d-1}) could be used instead of ê (P,Q) if desired.
- The approach of using a power of the Tate pairing that can be computed more efficiently was pioneered by Eisentraeger, Lauter and Montgomery in the form of squared pairings.

A simplified algorithm (finally)

- For p = 3 and a careful choice of the function $f_{p,\mathrm{P}}$, this gives the Duursma-Lee algorithm!
- The original derivation by Duursma and Lee used *ad hoc* properties of $f_{p,\mathrm{P}}$. The η pairing approach is more general (see forthcoming paper by Galbraith, Scott, and myself).
- Examples: elliptic and hyperelliptic curves in characteristic 2.

The Duursma-Lee algorithm

// $\sigma \in \mathbf{F}_{3^2}$, $\rho \in \mathbf{F}_{3^6}$: $\sigma^2 = -1$, $\rho^3 = \rho + b$.

$(\alpha, \beta) \leftarrow P$, $(x, y) \leftarrow Q$

$f \leftarrow 1$

for i $\leftarrow$ 0 **to** m–1 **do**

$\alpha \leftarrow \alpha^3$, $\beta \leftarrow \beta^3$

$\mu \leftarrow \alpha + x + b$, $\lambda \leftarrow -\beta \cdot y\sigma - \mu^2$

$g \leftarrow \lambda - \mu\rho - \rho^2$

$f \leftarrow f \cdot g$

$x \leftarrow x^{1/3}$, $y \leftarrow y^{1/3}$

end for

return f^{q^3-1} // $= \hat{e}(P,Q)$

Example in characteristic 2

// $s \in \mathbf{F}_{2^2}$, $t \in \mathbf{F}_{2^4}$: $s^2 = s + 1$, $t^2 = t + s$.

$(\alpha, \beta) \leftarrow$ P, $(x, y) \leftarrow$ Q

$f \leftarrow 1$

for i $\leftarrow$ 0 **to** m–1 **do**

  $u \leftarrow \alpha^2$

  $\mu \leftarrow u + x + 1$, $\lambda \leftarrow (u + 1)\cdot(\alpha + x) + u + \beta + y$

  $g \leftarrow \lambda + \mu s + t$

  $f \leftarrow f\cdot g$

  $\alpha \leftarrow u$, $\beta \leftarrow \beta^2$, $x \leftarrow x^{1/2}$, $y \leftarrow y^{1/2}$

end for

return $f^{\,q^2-1}$ // = ê(P,Q)

Example in characteristic 2

- Application to the hyperelliptic curve $y^2 + y = x^5 + x^3 + b$:
  - Embedding degree $k = 12$.
  - Efficient arithmetic (divisor octuplication formula analogous to point doubling or tripling).
  - Efficient pairing computation.
- More details? Read our forthcoming paper ☺

Interactive pairing-based schemes

- Several cryptographic schemes need to transmit or store pairing values, e.g.:
  - Baek-Zheng zero knowledge proof for the equality of two discrete logarithms.
  - Boneh-Boyen selective-id id-based encryption.
  - Chow et al. undeniable signature scheme.
  - Du et al. authenticated group key agreement scheme.
  - Nguyen's group signature scheme.
  - Scott's authenticated key agreement.
  - ... others.

Pairing compression

- Conventional algorithms account for efficient computation but not for bandwidth optimisation.
- Using traces enables compressing an $\mathbf{F}_{q^6}$ pairing value to an element of either $\mathbf{F}_{q^3}$ (compression rate 2:1) or $\mathbf{F}_{q^2}$ (compression rate 3:1).
- Alternative: torus-based algorithms (same compression rate and computational efficiency).

Pairing compression

- Duursma-Lee for $\mathbf{F}_{q^2}$ traces: simply take advantage of representing $\mathbf{F}_{q^6}$ as $\mathbf{F}_{q^2}[x]/(x^3-x-b)$ and $\mathbf{F}_{q^2}$ as $\mathbf{F}_q[x]/(x^2+1)$.
- Total cost is ~15m $\mathbf{F}_q$ multiplications (or ~14m with loop unrolling), neglecting the cost of cube roots and simpler operations.
- Final "powering" to q^3-1 (i.e. Frobenius plus inversion) performed on full $\mathbf{F}_{q^6}$ output before keeping only the $\mathbf{F}_{q^2}$ trace.

Pairing compression

- Further powering of pairing values as needed by cryptographic protocols may either use a ternary algorithm on the full $\mathbf{F}_{q^6}$ ladder output before truncation...
- ... or keep only the trace and use implicit exponentiation algorithms:
  - Ternary Lucas-like for $\mathbf{F}_{q^3}$ traces.
  - Ternary XTR-like ladder for $\mathbf{F}_{q^2}$ traces.

Effects of the pairing choice

- Distortion maps exist only for supersingular curves. Hence the Tate pairing is only available on ordinary curves in its reduced but unmodified form e(P,Q).
- It turns out that the choice between e(P,Q) or ê(P,Q) may lead to protocols with *different cryptographic properties*.

Effects of the pairing choice

- Example: McCullagh-Barreto identity-based authenticated key agreement protocol.
- Modified pairing $\Rightarrow$ escrowed system.
- Unmodified pairing $\Rightarrow$ escrowless scheme (unintuitive: identity-based schemes seem in general inherently escrowed).

Escrowed protocol

- Setup:
  - $\exists$ efficiently computable distortion map ψ: $E(\mathbf{F}_q) \rightarrow E(\mathbf{F}_{q^k})$.
  - KGC chooses $P \in_R E(\mathbf{F}_q)[r]$.
  - KGC chooses private key $s \in_R \mathbf{Z}_r^*$.
  - KGC publishes P and public key $V = sP$.
- Key Extraction:
  - User identity is $u \in \mathbf{Z}_r^*$.
  - KGC computes and delivers the user's private key as $U_{priv} = (u + s)^{-1}P$.

Escrowed protocol

- Key Agreement:
  - Alice: Bob:
  - $n_a \in_R \mathbf{Z}_r^*$ $n_b \in_R \mathbf{Z}_r^*$
  - $A_{KA} = n_a(bP + V) \rightarrow$ $\leftarrow n_b(aP + V) = B_{KA}$
  - $K = \hat{e}(B_{KA}, A_{priv})^{n_a}$ $K = \hat{e}(A_{KA}, B_{priv})^{n_b}$
- Escrow: KGC can retrieve $K = \hat{e}(P, P)^{n_a n_b} = \hat{e}(n_a P, n_b P)$ by computing:
  - $n_a P = (b + s)^{-1} A_{KA}$
  - $n_b P = (a + s)^{-1} B_{KA}$

Escrowless protocol

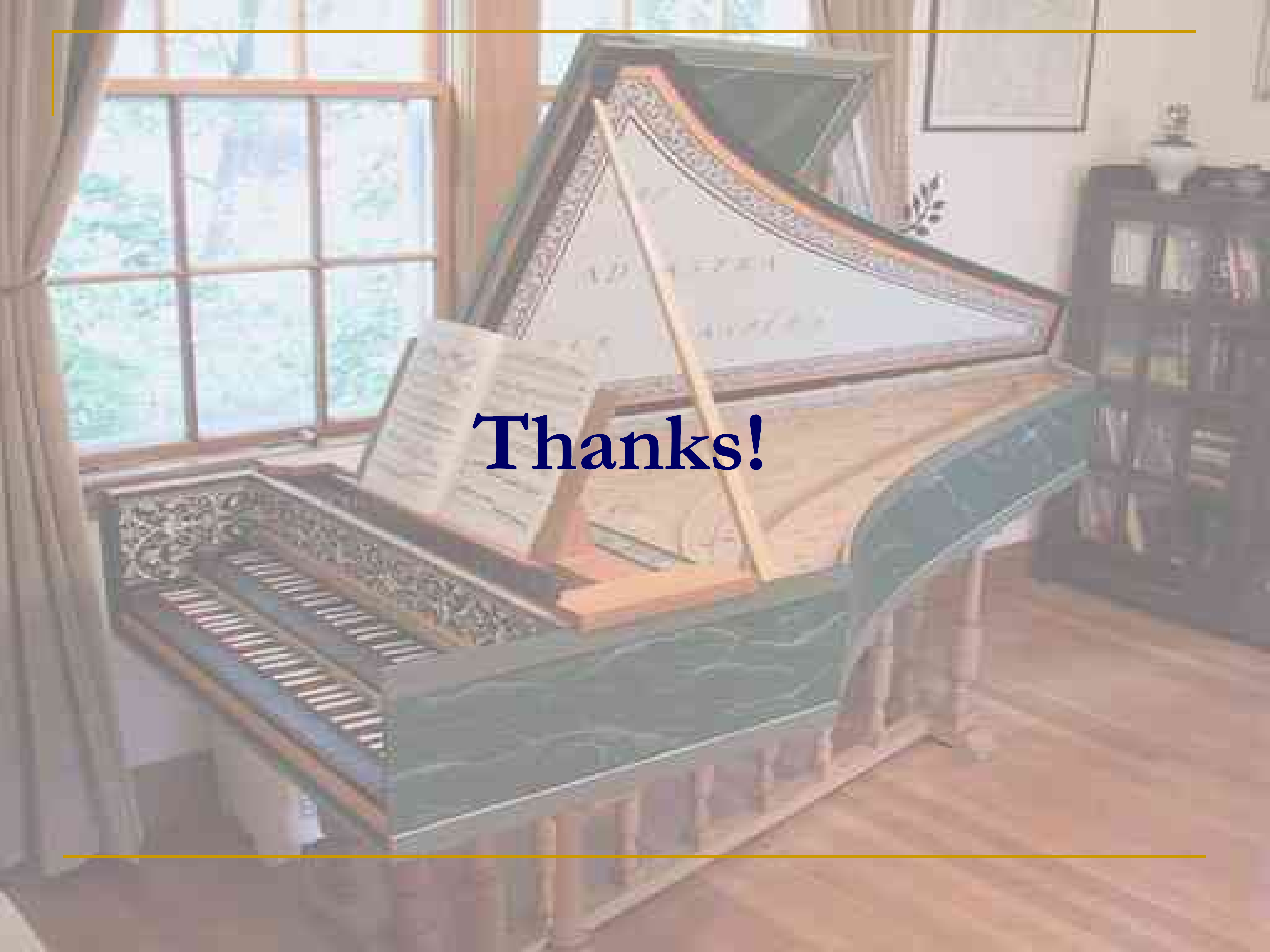
- Setup:
  - *No* efficiently computable distortion map ψ: $E(\mathbf{F}_q) \rightarrow E(\mathbf{F}_{q^k})$.
  - KGC chooses $P \in_R E(\mathbf{F}_q)[r]$, $Q \in_R E(\mathbf{F}_{q^k})$.
  - KGC chooses private key $s \in_R \mathbf{Z}_r^*$.
  - KGC publishes P, Q, and public key $V = sP$.
- Key Extraction:
  - User identity is $u \in \mathbf{Z}_r^*$.
  - KGC computes and delivers the user's private key as $U_{priv} = (u + s)^{-1}Q$.

Escrowless protocol

- Key Agreement:
  - Alice: Bob:
  - $n_a \in_R \mathbf{Z}_r^*$ $n_b \in_R \mathbf{Z}_r^*$
  - $A_{KA} = n_a(bP + V) \rightarrow$ $\leftarrow n_b(aP + V) = B_{KA}$
  - $K = e(B_{KA}, A_{priv})^{n_a}$ $K = e(A_{KA}, B_{priv})^{n_b}$
- No Escrow: the KGC can compute $e(P, Q)^{n_a}$ and $e(P, Q)^{n_b}$ using the technique of the escrowed version, but obtaining $e(P, Q)^{n_a n_b}$ from these values now involves solving the Computational DH problem.

Summary

- Generalized Duursma-Lee algorithm (extension to other characteristics and genera).
- Pairing compression.
- Effects of pairing choice upon the properties of cryptographic protocols.



Thanks!

References

- [Baek-Zheng]
  - J. Baek, Y. Zheng, “Identity-Based Threshold Decryption,” PKC’2004, LNCS 2947, Springer-Verlag (2004), pp. 262—276.
- [Barreto-Kim-Lynn-Scott]
  - P. S. L. M. Barreto, H. Y. Kim. B. Lynn, M. Scott, “Efficient Algorithms for Pairing-Based Cryptosystems,” Crypto'2002, LNCS 2442, Springer-Verlag (2002), pp. 354—368.
- [Boneh-Boyen]
  - D. Boneh, X. Boyen, “Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles,” Eurocrypt’2004, LNCS 3027, Springer-Verlag (2004), pp. 223—238.
- [Chow-Yiu-Hui-Chow]
  - S. S. M. Chow, S. M. Yiu, L. C. K. Hui, K. P. Chow, “Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity,” ICISC’2003, LNCS 2971, Springer-Verlag (2004), pp. 352—369.
- [Du-Wang-Ge-Wang]
  - X. Du, Y. Wang, J. Ge, Y. Wang, “ID-based Authenticated Two Round Multi-Party Key Agreement,” Cryptology ePrint Archive, Report 2003/247.

References

- [Duursma-Lee]
  - I. M. Duursma, H.-S. Lee, “Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$,” Asiacrypt'2003, LNCS 2894, Springer-Verlag (2003), pp. 111—123.
- [Eisentraeger-Lauter-Montgomery]
  - K. Eisentraeger, K. Lauter, P. L. Montgomery, “Improved Weil and Tate Pairings for Elliptic and Hyperelliptic Curves,” ANTS-VI, LNCS 3076, Springer-Verlag (2004), pp. 169—183.
- [Galbraith-Harrison-Soldera]
  - S. D. Galbraith, K. Harrison, D. Soldera, “Implementing the Tate pairing,” ANTS-V, LNCS 2369, Springer-Verlag (2002), pp. 324—337.
- [Granger-Page-Stam]
  - R. Granger, D. Page, M. Stam,, “On Small Characteristic Algebraic Tori in Pairing-Based Cryptography,” Cryptology ePrint Archive, Report 2004/132.
- [McCullagh-Barreto]
  - N. McCullagh, P. S. L. M. Barreto, “A New Two-Party Identity-Based Authenticated Key Agreement,” CT-RSA 2005, LNCS, Springer-Verlag, to appear.
- [Nguyen]
  - L. Nguyen, “A Trapdoor-free and Efficient Group Signature Scheme from Bilinear Pairings,” Cryptology ePrint Archive, Report 2004/104.