Notation

Basic mathematical notation

$\varnothing$	The empty set
$\#S$	The number of elements in the finite set S
$S - T$	Set difference of sets S and T
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	integers, rationals, reals and complex numbers
$\mathbb{N}$, $\mathbb{Z}_{>0}$	Natural numbers
$\mathbb{Z}/r\mathbb{Z}$	Integers modulo r
$\mathbb{F}_q$	Finite field of $q = p^m$ elements
$\mathbb{Z}_p$, $\mathbb{Q}_p$	p-adic ring, field, where p (sometimes also called l) is a prime.
$\langle g_1, \dots, g_n \rangle$	Group generated by $g_1, \dots, g_n$
$(g_1, \dots, g_n)$	Ideal generated over a ring R by $g_1, \dots, g_n \in R$
$\varphi(n)$	Euler phi function
$\zeta(n)$	Riemann zeta function
$\lambda(N)$	Carmichael lambda function
$a \mid b, a \nmid b$	b is/is not a multiple of a
q_n, r_n	Quotient and remainder in n-th step of Euclidean algorithm
s_n, t_n	Numbers arising in the extended Euclidean algorithm to compute $\gcd(a, b)$, they satisfy $r_n = as_n + bt_n$
h_n/k_n	Convergents of a continued fraction expansion
$\log_2(x)$	Logarithm to base 2
$\log(x)$	Natural logarithm
$[0, 1]$	$\{x \in \mathbb{R} : 0 \leq x \leq 1\}$
$\approx$	Approximately equal (we do not give a precise definition), such as $\pi \approx 3.1415$
$(a_{l-1} \dots a_1 a_0)_2$	Binary representation of an integer a
$\underline{v}, \underline{w}$	Vectors
$\underline{0}$	Zero vector
$\underline{e}_i$	i-th unit vector
I_n	$n \times n$ identity matrix
$\langle \underline{x}, \underline{x} \rangle$	Inner product
$\Vert \underline{x} \Vert$	Euclidean length of a vector (2 norm)
$\Vert \cdot \Vert_a$	ℓ_a-norm for $a \in \mathbb{N}$
$\mathrm{span}\{\underline{v}_1, \dots, \underline{v}_n\}$	Span of a set of vectors
$\mathrm{rank}(A)$	Rank of a matrix A
$M_n(R)$	$n \times n$ matrices over the ring R
$\lfloor x \rfloor$	Round $x \in \mathbb{R}$ down to an integer
$\lceil x \rceil$	Round $x \in \mathbb{R}$ up to an integer
$[x]$, $\lfloor x \rceil$	Closest integer to x, with $[1/2] = \lfloor 1/2 \rceil = 1$

Notation for polynomials and fields

$\mathbb{F}_q$	Finite field of $q = p^m$ elements
$F(x)$	Irreducible polynomial defining a finite field
θ	Generator of a finite field
$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$	Trace
$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ or N	Norm map with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$
$\Bbbk$	Ground field, always assumed to be perfect
$\mathrm{char}(\Bbbk)$	The characteristic of $\Bbbk$ (either 0 or a prime)
$\overline{\Bbbk}$	An algebraic closure of $\Bbbk$
$\Bbbk'$	A field extension of $\Bbbk$ contained in $\overline{\Bbbk}$
$\mathrm{Gal}(\Bbbk'/\Bbbk)$	Galois group if $\Bbbk'/\Bbbk$ is Galois
trdeg	Transcendence degree
$F(x)$	Polynomial of degree d
$F'(x)$	The derivative of the polynoial $F(x)$
$R(F, G), R_x(F(x), G(x))$	Resultant of polynomials
$R_1(x), R_i(x), T(x)$	Polynomials arising in polynomial factorisation algorithms of Section 2.12
$\deg(F(x)), \deg_x(F(x))$	Degree of polynomial
$\deg(f(\underline{x}))$	Total degree of polynomial
F	Polynomial in $\mathbb{F}_q[x]$ of degree m defining $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/(F(x))$
$\mathbb{Z}_F$	Ring of integers of number field F
$\mathrm{Cl}(\mathcal{O})$	Class group of order $\mathcal{O}$
$h(\mathcal{O})$	Class number of order $\mathcal{O}$

Notation for algorithms and complexity

$O(f)$	Big O notation
$o(f)$	Little o notation
$\tilde{O}(f)$	Soft O notation
$\Omega(f)$	Big Omega notation
$\Theta(f)$	Big Theta notation
$\leq_R$	Reduction
$\mathrm{len}(a)$	The bit-length of a
$\mathrm{wt}(m)$	The Hamming weight of m (number of ones in binary expansion)
$M(n)$	The cost of multiplication of two n-bit integers
$M(d, q) = M(d \log(dq))$	The cost of multiplying two degree d polynomials over $\mathbb{F}_q$
$s \leftarrow S$	$s \in S$ chosen according to an (implicit) distribution on S
$L_N(a, c)$	Subexponential function
O, A	Oracle

Notation for algebraic geometry

$G_a(\Bbbk)$	Additive group $(\Bbbk, +)$
$G_m(\Bbbk)$	Multiplicative group $(\Bbbk^*, .)$
mult	Multiplication map in an algebraic group
inverse	Inverse map in an algebraic group
$[g]$	Orbit or equivalence class of g under an automorphism
G/ψ	Set of orbits/equivalence classes of G under the automorphism ψ
$\mathbb{A}^n(\Bbbk)$	Affine space, points $(x_1, \dots, x_n)$
$\mathbb{P}^n(\Bbbk)$	Projective space, points $(x_0 : \dots \vert x_n)$
$(x_0 : \cdots : x_n)$	Homogeneous coordinate for point of $\mathbb{P}^n$
$\equiv$	Equivalence of $(n+1)$-tuples to define projective space
$\underline{x}$	Either $(x_1, \dots, x_n) \in \mathbb{A}^n(\Bbbk)$ or $(x_0 : \cdots : x_n) \in \mathbb{P}^n(\Bbbk)$
X, Y	Algebraic set
$X(\Bbbk)$	$\Bbbk$-rational points of X

$V(I)$	Zero set of the ideal I
(S)	Ideal over $\Bbbk[\underline{x}]$ generated by the set S
$I_{\Bbbk}(X), I(X)$	Ideal over $\Bbbk$ corresponding to the algebraic set X over $\Bbbk$
$\mathrm{rad}(I)$	Radical of the ideal I
$\Bbbk[X]$	Coordinate ring of algebraic set X
$\Bbbk(X)$m $\Bbbk(C)$	Function field of X (resp. C)
F, K, L	Function field
U_i	Subset of $\mathbb{P}^n$ comprising all points $(x_0 : \cdots : x_n)$ with $x_i \neq 0$
φ_i	Rational map $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ with image U_i
φ	Rational map φ_n
φ_i^*	Homogenisation map from $\Bbbk[y_1, \ldots, y_n]$ to $\Bbbk[x_0, \ldots, x_n]$
φ_i^{-1}	Rational map $\mathbb{P}^n \to \mathbb{A}^n$
φ_i^{-1*}	De-homogenisation $\Bbbk[x_0, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n]$
$X \cap \mathbb{A}^n$	Abbreviation for $\varphi_n^{-1}(X \cap U_n)$
$\overline{f}$	Homogenisation of the polynomial f
$\overline{I}$	Homogenisation of the ideal I
$\overline{X}$	Projective closure of algebraic set $X \subseteq \mathbb{A}^n$
$\mathcal{O}(X)$	Regular functions on variety X
$\dim(X)$	Dimension of the algebraic variety X
ϕ	Rational map or morphism of varieties
$\mathfrak{p}$	A prime ideal of a ring
$S^{-1}R$	The localiation of a ring with respect to a multiplicative set S
$R_{\mathfrak{p}}$	The localisation of a ring at the prime ideal $\mathfrak{p}$
$\mathcal{O}_{P,\Bbbk}(X), \mathcal{O}_P$	Local ring of X at P.
$\mathfrak{m}_{P,\Bbbk}(X), \mathfrak{m}_P$	Maximal ideal of $\mathcal{O}_{P,\Bbbk}(X)$
$J_{X,P}$	Jacobian matrix of $X = V(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ at P
C	Curve
E	Elliptic curve
$C(\Bbbk)$, $E(\Bbbk)$	The $\Bbbk$-rational points of C (resp. E)
$\mathcal{O}_E, \mathcal{O}_C$	Point at infinity on a curve
$\iota(P)$	If $P = (x, y)$ then $\iota(P) = (x, -y - a_1x - a_3)$
$v_P(f)$	Valuation of function $f \in \Bbbk(C)$ at point P
t_P	Uniformizer at P
$l(x, y)$	Line between points P_1 and P_2 on an elliptic curve
$v(x)$	Vertical line on an elliptic curve
$\mathrm{Hom}_{\Bbbk}(E_1, E_2), \mathrm{End}_{\Bbbk}(E)$	Homomorphisms/endos of elliptic curves
$T_l(E)$	Tate module of an elliptic curve
$x(P), x_P, y(P), y_P$	Coordinates of the point $P = (x_P, y_P) \in C(\overline{\Bbbk})$
π_q	q-power Frobenius map
P_0	A given k-rational point on a curve
$\Phi_n(x)$	n-th cyclotomic polynomial
$G_{q,n}$	Cyclotomic subgroup of $\mathbb{F}_{q^n}^*$ of order $\Phi_n(q)$
g	An element of $G_{q,n}$
θ	Generator over $\mathbb{F}_q$ of a finite field $\mathbb{F}_{q^2}$
$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ or Tr	Trace map with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$
$\mathbb{T}_n$	Algebraic torus
comp	Torus compression function
decomp	Torus decompression function
$\star$	Partial group operation for $\mathbb{T}_2$

V_n	Trace of g^n in LUC
U	Hypersurface in the construction of $\mathbb{T}_6$
p_U	Rational parameterisation of the hypersurface U
$\chi_g(x)$	Characteristic polynomial over $\mathbb{F}_{q^2}$ of element of $\mathbb{F}_{q^6}$
t_n	Trace of g^n in XTR
$F(x), H(x)$	Polynomials in $\Bbbk[x]$ used to define a curve
$E(x,y)$	Weierstrass equation $y^2 + H(x)y - F(x)$
a_1, a_2, a_3, a_4, a_6	Coefficients of Weierstrass equation
D	Divisor
$\operatorname{div}(f)$	Divisor of the function f
$\operatorname{Supp}(D)$	Support of a divisor
$\operatorname{Div}_{\Bbbk}(C)$	Divisors on C defined over $\Bbbk$
$\operatorname{Div}^0_{\Bbbk}(C)$	Degree zero divisors on C defined over $\Bbbk$
$\operatorname{Prin}_{\Bbbk}(C)$	Principal divisors on C
$\overline{D}$	Divisor class
$\operatorname{Pic}^0_{\Bbbk}(C)$	Degree zero divisor class group of curve C over $\Bbbk$
$\equiv$	Linear equivalence (i.e., equivalence of divisors)
$v' \mid v$	Extension of valuations
R_v	Valuation ring
$\mathfrak{m}_v$	Maximal ideal of the valuation
$\mathcal{L}_{\Bbbk}(D)$	Riemann-Roch space for divisor D
$\ell_{\Bbbk}(D)$	Dimension of Riemann-Roch space for D
$D \leq D'$	Ordering relation on divisors
DivEff	Set of all effective divisors
$\operatorname{Pic}^d_{\Bbbk}(X)$	Divisor class group (degree d divisor class group of X over the field k)
$\deg_x a(x)$	Degree in x of the polynomial $a(x)$
$\deg(\phi)$	Degree of the morphism ϕ
$\deg(D)$	Degree of the divisor D
ϕ^*	Pullback under a morphism
ϕ_*	Pushforward under a morphism
g	genus of curve C
$\partial F/\partial x$	Standard partial differentiation of polynomials or rational functions
hdx	Differential on C
$\Omega_{\Bbbk}(C)$	Set of differentials on C over $\Bbbk$
ω	Differential on C
ω_E	Invariant differential on elliptic curve E
$\operatorname{div}(\omega)$	Divisor of a differential on C
$(C,P), (E,O)$	A *pointed curve*, i.e., a curve over $\Bbbk$ together with a specified $\Bbbk$-rational point.
τ_Q	Translation map
$[n]$	Multiplication by n map on an elliptic curve (or torus or Abelian variety)
$E[n]$	Points of order dividing n on an elliptic curve
$\operatorname{Twist}(E)$	Set of classes of twists of E
$E^{(d)}$	Quadratic twist of E
$\operatorname{Hom}_{\Bbbk}(E_1, E_2)$	Group of isogenies from E_1 to E_2 over $\Bbbk$
$\operatorname{End}_{\Bbbk}(E)$	Ring of isogenies from E to itself over $\Bbbk$
$\ker(\phi)$	Kernel of an isogeny
t_∞	Uniformizer on elliptic curve at $\mathcal{O}_E$
$P(T)$	Characteristic polynomial of Frobenius

$\hat{\phi}$	Dual isogeny
$\deg_s(\phi)$	Separable degree
$\deg_i(\phi)$	Inseparable degree
$(Y : X_d : \cdots : X_0)$	Variables for projective non-singular equation of hyperelliptic curve
$C^\dagger$	Image of hyperelliptic curve C under map swapping ∞ and zero
ρ_P	Birational map from hyperelliptic curve taking P to infinity
$(u(x), v(x))$	Mumford representation for semi-reduced divisors
∞^+, ∞^-	Points at infinity on a hyperelliptic curve
$\mathrm{monic}(u(x))$	Monic polynomial obtain by dividing by the leading coefficient
$\mathrm{div}(u(x), y - v(x))$	Greatest common divisor of $\mathrm{div}(u(x))$ and $\mathrm{div}(y - v(x))$
$u^\dagger, v^\dagger, v^\ddagger$	Polynomials arising in Cantor reduction and reduction at infinity
$D^\dagger$	Semi-reduced divisor arising from Cantor's reduction
D_∞	Effective Divisor on a hyperelliptic curve of degree g with support only at infinity
$(u(x), v(x), n)$	Divisor $\mathrm{div}(u(x), y - v(x)) \cap \mathbb{A}^2 + n(\infty^+) + (g - \deg(u(x)) - n)(\infty^-)$
J_C	Jacobian variety of the curve C
Θ	Mumford theta divisor
$L(t)$	L-polynomial of the curve C over $\mathbb{F}_q$
α_i	Roots of $P(T)$ and reciprocal roots of $L(t)$ for curve C over $\mathbb{F}_q$
$\mathbb{K}/\Bbbk$	Fields in Weil descent attack

Notation for algorithms in algebraic groups

NAF	Non-adjacent form
w-NAF or NAF_w	Width w non-adjacent form
$\mathcal{D}$	Digit set for an expansion
digit	Function assigning to an integer and integer in $\mathcal{D}$
weight	Weight of the expansion
$\log_g(h)$	Discrete logarithm problem ($g \in G$)
r	Large prime, the order of $g \in G$
$\pmod{\mathrm{s}\ m}$ (mods m)	Modular reduction to signed residue
$\overline{1}$	Coefficient -1 in a signed expansion
PH	Pohlig-Hellman algorithm
BSGS	Baby-step-giant-step algorithm
$\mathcal{S}_j$	Sets for representation problem and product DLP
L_j	Lists for generalised birthday algorithm
LSB_m	m least signficant bits
MSB_m	m most signficant bits, or bits specifying a decomposition of the domain into equal partitions
HNP	Hidden number problem

Notation in Chapter 14

G	An algebraic group or algebraic group quotient
g	An element in an AG or AGQ G, usually of prime order r
r	The prime order of an element g
h	An element in $\langle g \rangle$
a	The discrete logarithm of h with respect to g
$\mathcal{S}$	A set
N	Size of the set $\mathcal{S}$, or an integer to be factored
$\pi(X)$	The number of primes $\leq X$
Pr	Probability
$\neg E$	Complemenent of an event E

l	The number of elements sampled from $\mathcal{S}$
n_S	Number of partitions in Pollard walk
S	Map from G to $\mathbb{Z}/n_S\mathbb{Z}$
$b(g)$	Binary representation of $g \in G$
X	Random variable
x_i	Random walk sequence
(a_i, b_i)	Representation of walk element $x_i = g^{a_i} h^{b_i}$
(u_j, v_j)	Powers of g and h in random walk steps
g_j	A jump in the random walk
walk	The random walk function
l_t	Length of tail of Pollard rho walk
l_h	Length of cycle (or head) of Pollard rho walk
ϵ	A small positive real number
$\mathcal{D}$	Set of distinguished points
n_D	Number of bits used to define distinguishing property
θ	Probability that a random $g \in G$ is a distinguished point
N_P	Number of processors
n	Number of steps made by tame kangaroo
type	Indicator 'tame' or 'wild'
s	Spacing between starting positions of kangaroos in the same herd
N_C	Size of generic equivalence class
$\overline{x}$	Equivalence class of x
$\hat{x}$	Equivalence class representative of class of x
$\mathrm{Aut}(G)$	Automorphism group of an algebraic group G
b	Start of interval; usually set to 0
w	Length of interval
m	Mean step size
$f : \mathcal{S} \to \mathcal{S}$	Function in parallel collision search
$f_i : \mathcal{S}_i \to \mathcal{R}$	Function in meet-in-the-middle attack
I	Set $\{0, 1, \ldots, N-1\}$
$\sigma_i : I \to \mathcal{S}_i$	Functions in parallel meet-in-middle-attack
$\rho : \mathcal{R} \to I \times 1, 2$	Function in parallel meet-in-middle-attack
$f(x)$	Function in Pollard rho factoring

Notation in Chapter 15

$\Psi(X, Y)$	Number of Y-smooth integers less than X
$f(n) \sim g(n)$	If $\lim_{n\to\infty} f(n)/g(n) = 1$
$\rho(u)$	Dickman-de Bruijn function
T_B	Expected number of trials until a random integer $1 \leq x < N$ is B-smooth
$L_N(a, c)$	Subexponential function
$\mathcal{B}$	Factor base
B	Bound on primes to define $\mathcal{B}$
s	Number of elements in factor base $\mathcal{B}$
$I(n)$	number of irreducible polynomials of degree n
$N(n, b)$	number of b-smooth polynomials of degree exactly equal to n
$p(n, b)$	probability that a uniformly chosen polynomial of degree at most n is b-smooth
$\mathrm{Summ}_n(x_1, \ldots, x_n)$	Summation polynomial

Notation for Part IV

$\underline{b}, \underline{v}, \underline{w}$	Row vectors (usually in $\mathbb{R}^m$)
$\underline{0}$	Zero vector in $\mathbb{R}^m$
$\underline{e}_i$	i-th unit vector in $\mathbb{R}^m$
I_n	$n \times n$ identity matrix
$\langle \underline{x}, \underline{x} \rangle$	Inner product
$\Vert \underline{x} \Vert$	Euclidean length (ℓ_2 norm)
$\Vert \cdot \Vert_a$	ℓ_a-norm for $a \in \mathbb{N}$
$\mathrm{span}\{\underline{v}_1, \dots, \underline{v}_n\}$	Span of a set of vectors over $\mathbb{R}$
$\mathrm{rank}(A)$	Rank of a matrix A
$\lfloor x \rceil$	Closest integer to x, $\lfloor 1/2 \rceil = 1$
B	Basis matrix for a lattice
L	Lattice
$\underline{b}_i^*$	Gram-Schmidt vector arising from ordered basis $\{\underline{b}_1, \dots, \underline{b}_n\}$
$\mu_{i,j}$	Gram-Schmidt coefficient $\langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$
B_i	$\Vert \underline{b}_i^* \Vert^2$
λ_i	Successive minima of a lattice
$\det(L)$	Determinant of a lattice
γ_n	Hermite's constant
X	Bound on the size of the entries in the basis matrix L
$B_{(i)}$	$i \times m$ matrix formed by the first i rows of B
d_i	Determinant of matrix of $\langle \underline{b}_j, \underline{b}_k \rangle$ for $1 \leq j, k \leq i$
D	Product of d_i
$\mathcal{P}_{1/2}(B)$	Fundamental domain (parallelepiped) for lattice basis B
$F(x)$, $F(x,y)$	Polynomial with "small" root
$G(x), G(x,y)$	Polynomial with "small" root in common with $F(x)$ (resp., $F(x,y)$)
X, Y	Bounds on size of root in Coppersmith's method
b_F	Coefficient vector of polynomial F
$R(F,G), R_x(F(x), G(x))$	Resultant of polynomials
W	Bound in Coppersmith's method
P, R	Constants in noisy Chinese remaindering
$\mathrm{amp}(x)$	The amplitude $\gcd(P, x-R)$ in noisy Chinese remaindering
B, B'	Basis matrices for GGH encryption
I_n	$n \times n$ identity matrix
U	Invertible matrix disguising the private key in GGH
$\underline{m}, \underline{e}, \underline{c}$	Message (respectively, error vector, ciphertext) in McEliece or GGH
σ	Entry in error vector in GGH
M	Size of coefficients in message in GGH
$\underline{s}$	GGH signature
$a_1, \dots, a_n$	Subset sum weights
$b_1, \dots, b_n$	Superincreasing sequence
$s = \sum_{i=1}^n x_i a_i$	The sum in a subset sum instance, with $x_i \in \{0,1\}$
d	Density of a subset sum instance
π	Permutation of $\{1, \dots, n\}$ used in the Merkle-Hellman cryptosystem
$\underline{\sigma}$	Vector in Nguyen attack
M	Modulus in Merkle-Hellman knapsack
W	Multiplier in Merkle-Hellman knapsack
U	$W^{-1} \pmod{M}$ in Merkle-Hellman
t	Number of iterations in iterated Merkle-Hellman knapsack

Notation for cryptography

κ	Security parameter
M	Message space
PK	Public key space
SK	Private key space
C	Ciphertext space
pk	Public key
sk	Private key
m	Message
c, $(\mathsf{c}_1, \mathsf{c}_2)$	Ciphertext
s, $(\mathsf{s}_1, \mathsf{s}_2)$	Signature
Enc	Symmetric encryption
Dec	Symmetric decryption
g	Element of an algebraic group G
$\perp$	Symbol for invalid ciphertext or algorithm failure
H	Cryptographic hash function
q_S	Number of signature queries in security proof
$F(s_1)$	Function used in Elgamal and DSA signatures
DLP	Discrete logarithm problem
CDH	Computational Diffie-Hellman problem
DDH	Decisional Diffie-Hellman problem
kdf	Key derivation function
Inverse-DH	Inverse Diffie-Hellman problem $(g, g^a) \mapsto g^{a^{-1}}$
Static-DH	Static Diffie-Hellman problem
Strong-DH	Strong Diffie-Hellman problem
Square-DH	Square Diffie-Hellman problem
Hash-DH	Hash Diffie-Hellman problem
Adv	Advantage of an algorithm
MAC	Message authentication code
KEM	Key encapsulation mechanism
DEM	Date encapsulation mechanism
$\mathcal{K}$	Key space (for a KEM)
$\mathcal{X}_{g_1,g_2,h}$	A set used in the security proof of the Cramer-Shoup encryption scheme
id	Identity of a user
S	The set of RSA moduli

Notation used in Part VII

E/G	Quotient elliptic curve by subgroup G
$\Phi_d(x, y)$	Modular polynomial
$\tilde{j}$	j-invariant of isogenous curve in Elkies method
$\mathfrak{a}, \mathfrak{b}, \mathfrak{l}$	$\mathcal{O}$-ideals
$X_{E,\mathbb{F}_q,S}$	Isogeny graph
$E[\mathfrak{l}]$	Kernel of isogeny corresponding to ideal $\mathfrak{l}$
$\delta_v(S)$	Vertex boundary of a set S in a graph
$\delta_e(S)$	Edge boundary of a set S in a graph
$f(D)$	Evaluation of function f at divisor D
e_n	Weil pairing
t_n	Tate-Lichtenbaum pairing
$\hat{t}_n$	Reduced Tate-Lichtenbaum pairing
$k(q, n)$	Embedding degree
G_1, G_2	Eigenspaces of Frobenius in $E[r]$
T	$t - 1$, used in the ate pairing
$a_T(Q, P)$	Ate pairing