CR3 Crittografia 3

A.A. 2008/2009

Prof. Francesco Pappalardi

Crittosistemi sulle Curve Ellittiche

1. Teoria delle Curve Ellittiche

L'equazione di Weierstrass, La struttura di gruppo sui punti razionali, formule per la somma e la duplicazione. Richiami sullo spazio proiettivo e sui polinomi omogenei, Il punto all'infinito di un'equazione di Weierstrass. Equazioni parametriche delle rette proiettive. Molteplicità di intersezione tra retta e curva nel piano proiettivo. Retta tangente. Punti singolari. Generalità sulla Teoria classica delle curve proiettive. Definizione di invariate j di una curva ellittica, curve ellittiche con invariante $j = 0, 1728$, proprietà dell'invariante j. Altre equazioni per curve ellittiche, Equazione di Legendre, Equazioni cubiche, Equazioni quartiche, intersezioni di due superfici cubiche. L'invariante j, curve ellittiche in caratteristica 2, curve singolari, curve ellittiche modulo n.

2. Punti di Torsione

Endomorfismi e proprietà degli endomorfismi. Separabilità. Nucleo degli endomorfismi separabili. Conseguenze. Criteri di separabilità. Punti di torsione, Polinomi di divisione. L'accoppiamento di Weil.

3. Curve ellittiche su campi finiti

L'endomorfismo di Frobenius e sue proprietà. Enunciato del Teorema di Waterhouse e di Ruck. Il Teorema di Hasse. Polinomio caratteristico dell'endomorfismo di Frobenius. Il problema di determinare l'ordine del gruppo. Curve su sottocampi, Simboli di Legendre, Ordini dei punti, L'algoritmo "Baby Step, Giant Step" di Shanks. Famiglie particolari di curve ellittiche. L'algoritmo di Schoof. La nozione di curva twist. Teoremi vari sulla struttura del gruppo dei punti razionali: Teorema di Mestre.

4. Crittosistemi sulle Curve Ellittiche

Il problema del Logaritmo Discreto. Algoritmi per il calcolo del logaritmo discreto: Baby-Step Giant-Step e Polig-Hellman. Attacco MOV. Attacco sulle curve anomale. Scambio di Chiavi di Diffie-Hellman. Crittosistemi di Massey Omura e El Gamal. Schema di Firma di El Gamal. Crittosistemi sulle curve ellittiche basati sul problema della fattorizzazione. Fattorizzzione di numeri interi utilizzando le curve ellittiche. Utilizzo di Pari.

Testi consigliati

[1] Lawrence C. Washington, *Elliptic Curves: Number Theory and Crptography*. Chapman & Hall (CRC), (2003).
[2] Alfred J. Menezes, *Elliptic Curve Public Key Cryptosystems, The Kluwer International Series in Engineering and Computer Science, Vol. 234*. Kluwer, (1993).

Bibliografia supplementare

[3] Darrel Hankerson, Alfred J. Menezes e Scott Vanstone, *Guide to Elliptic Curve Cryptography*. Springer Professional Computing, (2004).
[4] Michael Rosing, *Implementing Elliptic Curve Cryptography*. Manning Greenwich, (1998).
[5] Ian Blake, Gadiel Seroussi e Nigel Smart, *Elliptic Curves in Cryptography*. Cambridge University Press, (1999).
[6] Andreas Enge, *Elliptic Curves and Their Applications to Cryptography. An Introduction*. Springer Verlag, (1999).

Modalità d'esame

- valutazione in itinere ("esoneri")		☐ SI	■ NO
- esame finale	scritto	■ SI	☐ NO
	orale	■ SI	☐ NO
- altre prove di valutazione del profitto (meglio descritte sotto)		■ SI	☐ NO

Si propone che gli studenti espongano dei seminari concordati con i docenti e che svolgano una serie di esercizi a casa. Per i dettagli consultare la pagina web:
http://www.mat.uniroma3.it/users/pappa/CORSI/CR3_08_09/CR3.htm.