DH via ECDLP in ECC!

di PASQUALINA FRAGNETO *e* BEATRICE ROSSI

Simboli strani: equazioni matematiche o sigle misteriose? Non vi preoccupate: il caldo estivo non ci ha dato alla testa! Nelle prossime pagine vi aiuteremo a decifrare il messaggio contenuto nel titolo!

ECC non sta per eccetera, ma per *Elliptic Curve Cryptography*, cioè crittografia delle curve ellittiche. Bene o male, vi sarete già imbattuti nella crittografia: se ne è già parlato anche in vari numeri di *XlaTangente* come ad esempio nel 6 e nel 7/8, e più recentemente nel 32 grazie allo scrittore Marco Malvaldi (pp. 23-25).

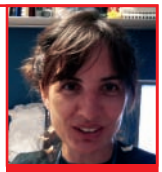
Probabilmente non tutti voi sapete, però, che cosa è una curva ellittica, anche perché per la ECC si usano le curve ellittiche su campi finiti GF(q), dove q è una potenza di un numero primo. Avete visto come è facile imbattersi in GF(3) a partire dal gioco SET alle pagine 11-13. Forse non eravate a conoscenza del fatto che il campo finito GF(2) viene utilizzato per i codici a barre, come mostra Elisabeth Busser nell'articolo alle pagine 14-15.

Sicuramente è affascinante il modo in cui possiamo fare geometria su un campo finito. E per geometria intendiamo proprio rette, curve e così via! Infatti, siamo abituati a pensare che questi enti geometrici siano continui e in questo caso non lo sono affatto! D'altra parte, essendo il campo su cui si fa la geometria un campo finito, non abbiamo più a che fare con enti che possiamo visualizzare come quelli usuali.

Prendiamo, ad esempio, l'insieme delle terne di numeri in GF(2). Abbiamo a che fare con un insieme, A^3, di 8 terne, cioè (0,0,0), (0,0,1), (0,1,1), (1,0,0), (0,1,0), (1,1,0), (1,0,1) e (1,1,1). Queste terne possono essere sommate tra loro componente per componente: la somma di (1,1,0) e (0,1,1) è (1,0,1) perché in GF(2) ricordiamo che 1 + 1 = 0. Pertanto A^3 ha una struttura lineare in quanto la somma di due suoi elementi è ancora un elemento di A^3.

Prendiamo ora in considerazione tutti i punti di A^3 tranne (0,0,0). Sono 7 punti che hanno una struttura geometrica chiamata "piano di Fano" dal geometra italiano Gino Fano (1871-1952). I sette punti stanno su sette rette:

Pasqualina Fragneto
Laureata in Matematica presso l'Università Federico II di Napoli nel 1998, è responsabile dal 2008 di un piccolo gruppo di ricerca in Matematica presso la STMicroelectronics. Si occupa di tecniche di ottimizzazione numerica e di studi di geometria proiettiva applicata alla *computer-graphics*.
pasqualina.fragneto@st.com



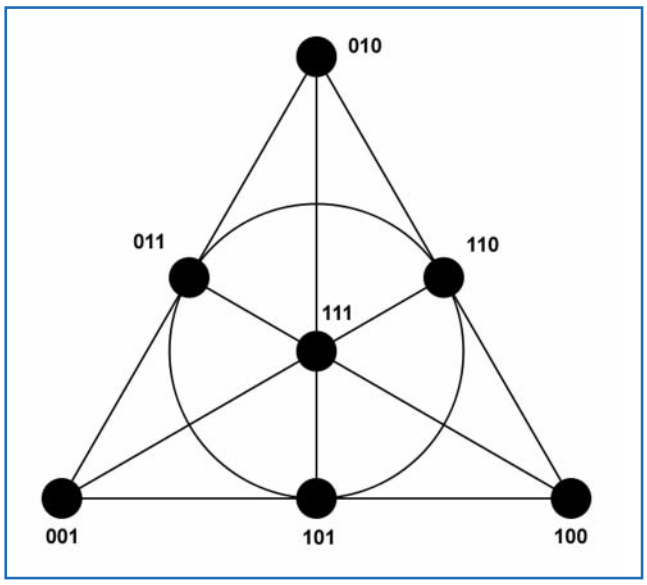
Beatrice Rossi
Laureata in Matematica presso l'Università degli Studi di Milano-Bicocca, lavora presso la STMicroelectronics. Si occupa di crittografia e di altri aspetti della matematica applicata, come la *computer-vision* e il *compressed-sensing*.
beatrice.rossi@st.com

Il piano proiettivo

Il piano di Fano è un *toy model* per il concetto di piano proiettivo su un qualsiasi campo finito GF(q); esso risulta formato da un insieme di punti e un insieme di rette tali che

1) per due punti qualsiasi passa un'unica retta;
2) due rette qualsiasi si incontrano in un unico punto;
3) esistono quattro punti tali che, comunque se ne scelgano tre, questi non risultano allineati.

Per dare un esempio basta prendere le rette per l'origine nello spazio delle terne su GF(q). Ci sono $q^3 - 1$ punti diversi dall'origine e, quindi, $q^3 - 1$ rette contate $q - 1$ volte, dato che su ognuna di esse (come in figura) ci sono $q - 1$ punti diversi dall'origine.



Il piano di Fano: in evidenza i 7 punti e le 7 rette di cui una appare... curva!

x = 0, y = 0, z = 0, x + y = 0, x + z = 0, y + z = 0, x + y + z = 0,

ciascuna delle quali è un sottoinsieme di 3 punti. Inoltre tre rette qualsiasi si incontrano in un solo punto ed esistono quattro punti tali che, comunque se ne scelgano tre, questi non risultano allineati – ad esempio, (1,0,0), (1,0,1), (1,1,0), (1,1,1).

Come abbiamo definito le rette, possiamo definire gli insiemi di punti che soddisfano equazioni di grado superiore, come le coniche (equazioni di grado 2) o le cubiche (equazioni di grado 3).
Una curva ellittica su un campo finito GF(q) è l'insieme dei punti (x,y,z) nel piano proiettivo sopra GF(q) che soddisfano un'equazione del tipo

$$y^2z + axyz + byz^2 - x^3 + cx^2 + dxz^2 + ez^3 = 0,$$

dove a,b,c,d,e, sono elementi del campo GF(q).

Ad esempio, consideriamo la curva $y^2z + x^3 + z^3 = 0$ su GF(2). Una prima possibilità per capire quali sono i punti di questa curva è quella di prendere i punti del piano proiettivo su GF(2) e di "sostituirli" uno ad uno. Si tratta di un metodo esplicito ma per campi grandi, come quelli che si usano nelle applicazioni, implica un grosso dispendio di energia. Il fatto di cercare un metodo alternativo ha costretto l'intera comunità di matematici a un grande sforzo, tuttora in corso, per capire le proprietà con cui determinare punti su curve ellittiche.

Torniamo al nostro esempio. Se z = 0, allora è x = 0, quindi il punto (0,1,0) appartiene alla curva. Se z è diverso da zero, allora z = 1. Si ha così:

$$y^2 + x^3 + 1 = 0.$$

Quali sono le soluzioni su GF(3)? Ve lo lasciamo come passatempo :-)

ECDLP sta per *Elliptic Curve Discrete Logarithm Problem*, ovvero il problema del logaritmo discreto su una curva ellittica. Una curva ellittica non è soltanto un oggetto geometrico in un piano proiettivo. Ha una struttura più ricca, ovvero di gruppo abeliano. L'insieme dei numeri interi con la somma è un gruppo abeliano perché la somma associa a due numeri interi un altro numero intero. La somma è associativa e lo 0 non altera il risultato se sommato ad altri interi. Inoltre ogni numero ha un opposto e la somma è commutativa (per questa ultima proprietà il gruppo si dice abeliano).

Incredibilmente, su una curva ellittica si può definire una somma come quella tra due numeri interi, una somma per cui a due punti della curva viene associato un terzo punto sempre della stessa curva. Esiste anche un elemento che si comporta come lo 0, che è un punto "speciale" indicato con O (in particolare, per ogni punto Q esiste un punto (–Q) che chiamiamo opposto tale che Q + (–Q) = O). L'operazione tra punti è puramente geometrica e può anche essere descritta mediante delle formule (che qui non riportiamo) nei termini delle coordinate con cui viene scritta un'equazione della curva ellittica. Dato un punto Q e un intero k, scriviamo kQ se Q + Q + ... + Q k volte Q se k è positivo; 0Q= O; e se k è negativo si pone kQ=(-k)(–Q), dove (–Q) è l'opposto di Q.

Dati k e Q, risulta relativamente semplice calcolare kQ mediante le formule di addizione. Viceversa, dati due punti qualsiasi T e R, si pone il problema di stabilire se esiste un intero k tale che T=kR. Tale problema è noto come "problema del logaritmo discreto su curve ellittiche". Il termine logaritmo discreto ha una genesi in teoria dei gruppi (vedi il box qui sotto).

Il problema del logaritmo

Sia Z il gruppo degli interi con l'usuale addizione. Fissiamo un numero *a* reale maggiore di zero. Non c'è differenza, se non nella notazione, tra Z e il gruppo di numeri reali positivi E(Z):= {a^n : n in Z} rispetto all'usuale moltiplicazione. Infatti l'operazione in E(Z) è data da a^n x a^m = a^{n+m} e l'elemento neutro è a^0. Dati due elementi a^n e a^m in E(Z), il numero intero k tale che a^n = $(a^m)^k$ può essere interpretato come l'esponente a cui elevare a^m per ottenere a^n, cioè il logaritmo in base a^m di a^n. Per questo si parla di logaritmo. L'aggettivo discreto deriva dal fatto che k è un intero.

Nel 1985, i matematici Miller e Koblitz ipotizzarono che un crittosistema basato sul logaritmo discreto potesse assicurare un livello di sicurezza molto elevato.
Questo è vero, perché il logaritmo discreto è considerato un problema intrattabile, cioè molto difficile da risolvere. In altri termini, è molto improbabile riuscire a trovare una formula risolutiva per il logaritmo discreto; l'unica possibilità è quella di provare, con un approccio che si chiama "a forza bruta", tutti i possibili esponenti.
In particolare, la sicurezza del crittosistema di Miller e Kobliz si basava sul fatto che, per riuscire a ricavare la chiave per la decifrazione, era necessario risolvere il problema del

Chiavi pubbliche e private

La crittografia a chiave pubblica è un sistema che richiede due chiavi separate, una per codificare un messaggio e l'altra per decodificarlo. Una di queste chiavi viene resa pubblica e l'altra viene tenuta privata. Se viene resa pubblica la chiave per codificare, allora il sistema consente di comunicare privatamente con il possessore della chiave privata. Se, invece, la chiave per decodificare è quella pubblica, il sistema serve come autenticazione di documenti cifrati da parte del possessore della chiave privata.

logaritmo discreto in un gruppo abbastanza grosso. In tale gruppo provare tutti gli esponenti diventava un'operazione lunghissima che avrebbe scoraggiato gli avversari sulla possibilità di trovare la soluzione in un tempo utile.
Miller e Kobliz si accorsero che lavorando con le curve ellittiche era possibile utilizzare chiavi per la cifratura e la decifrazione dei messaggi che avessero un numero minore di *bit*, ma che allo stesso tempo assicurassero lo stesso livello di sicurezza dei sistemi tradizionali.
Era chiaro inoltre che per i loro scopi Miller e Kobliz dovevano usare delle curve che potessero essere ben rappresentate tramite l'aritmetica finita dei calcolatori, e proprio per questo scelsero delle curve definite su campi finiti.

Se i sistemi che basano la propria sicurezza sull'ECDLP furono accolti con entusiasmo dalla comunità scientifica, ciò non avvenne però nel mondo dell'industria.

Al fine di aumentare la conoscenza e l'apprezzamento da parte delle aziende di questi nuovi sistemi e di stimolare ulteriori ricerche sull'analisi in termini di sicurezza, la Certicom, una società canadese che lavora nel campo della crittografia e della sicurezza delle comunicazione *wireless* (ossia senza cavo), ha introdotto nel 1997 *The Certicom ECC challenge* (La sfida Certicom ECC).

La sfida consiste nel calcolare le chiavi private ECC da un dato elenco di chiavi pubbliche ECC e dai relativi parametri di sistema, ovvero le caratteristiche della curva. Questo è il tipo di problema che deve affrontare un avversario che vuole sconfiggere completamente un sistema di crittografia su curve ellittiche.
La sfida, in realtà, è molto più articolata. Essa consiste in tre esercizi preparatori, con chiavi da 79, 89 e 97 *bit*, e da due livelli di sfida vera e propria.
Il primo livello prevede una difficoltà superabile solo con un massiccio impiego di potenza di calcolo, con chiavi da 109 e 131 *bit*.
Il secondo livello è previsto con chiavi di lunghezza tale da essere pressoché inattaccabili a livello computazionale, con lunghezze da 163, 191, 239 e 359 *bit*.

Nel 2002 e nel 2004 le sfide riguardanti 2 chiavi di 109 *bit* sono state risolte; nel primo caso, la curva ellittica era definita sul campo GF(2^m) e una squadra di matematici ha utilizzato una massiccia quantità di potenza di calcolo tra cui 10.000 computer (per lo più PC) in esecuzione 24 ore al giorno per 549 giorni. Lo stesso gruppo di matematici ha affrontato la sfida di secondo livello, cioè ha cercato di ricavare la chiave privata ECC partendo dalla conoscenza della chiave pubblica e dai parametri di sistema nel caso in cui la curva fosse definita su un campo finito GF(p). Ci sono riusciti nel 2004 con 2600 computer e dopo 17 mesi di calcolo.
Ad oggi risulta che la sfida successiva ECC a 131 *bit* non sia ancora stata vinta da nessuno (http://www.certicom.com/index.php/the-certicom-ecc-challenge).

Questo significa che la ECC con chiavi a più di 131 *bit* può essere considerata sicura e usata a livello industriale.

DH sta per Diffie e Hellman, un matematico e un informatico che nel 1976 hanno introdotto il sistema a chiave pubblica, il primo metodo pratico per due interlocutori di accordarsi su un segreto condiviso (la chiave) utilizzando un canale di comunicazione non protetto.

Il protocollo Diffie-Hellman è utilizzato per la negoziazione di una chiave tra due utenti, che vogliono comunicare mediante uno schema simmetrico di cifratura. Idealmente dovrebbe esistere un canale sicuro lungo il quale i due utenti, chiamiamoli per semplicità Mimì e Cocò, possano scambiarsi la chiave segreta. In assenza di un canale con questa caratteristica, si può ripiegare su un canale insicuro, applicando però il seguente protocollo:

1) Mimì e Cocò concordano pubblicamente sull'impiego di una curva ellittica su GF(p) e di un punto a coordinate in GF(p) appartenente alla curva ellittica;
2) Mimì sceglie una chiave segreta come un numero casuale $k_{s,B} \in [1, n-1]$, dove n rappresenta il numero dei punti della curva ellittica;
3) Cocò sceglie una chiave segreta come un numero casuale $k_{s,A} \in [1, n-1]$;
4) Mimì calcola $P_B = k_{s,B}P$ e lo invia a Cocò;
5) Cocò calcola $P_A = k_{s,A}P$ e lo invia a Mimì;
6) Entrambi sono in grado di calcolare una chiave comune per la comunicazione con il seguente procedimento:
• Mimì, usando il messaggio ricevuto, calcola
$P_{BA} = k_{s,B}P_A = k_{s,B} \cdot k_{s,A}P$;
• Cocò, usando il messaggio ricevuto, calcola
$P_{AB} = k_{s,B}P_B = k_{s,A} \cdot k_{s,B}P$;

In conclusione, Mimì e Cocò dispongono di uno stesso valore $P_{AB} = P_{BA}$ che potrà essere utilizzato come chiave comune per la comunicazione. Nel caso in cui un avversario, Oscar, intercetti entrambi i messaggi $P_B = k_{s,B}P$ e $P_A = k_{s,A}P$, anche conoscendo tutti i parametri della curva ellittica utilizzata, egli non riesce a determinare la chiave di sessione $P_{AB} = P_{BA}$ senza conoscere una delle due chiavi segrete; ma queste ultime non sono ricavabili da P_B e P_A grazie all'intrattabilità di ECDLP.
Così, il risultato finale non è assolutamente ricavabile da uno solo dei due partecipanti, senza il contributo dell'altro.