UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

PRIMO WORKSHOP DI CRITTOGRAFIA "BUNNYTN" 2011

Giovedì 10 marzo 2011
Aula 222 Polo Ferrari
Facoltà di Scienze – Università di Trento

PROGRAMMA:

9:00 – 9:10	**Presentazione del workshop** *Prof. Massimiliano Sala,* Università di Trento.
9:10 – 9:40	**Sui reticoli ibridi e il crittosistema NTWO** *Dott.ssa Emmanuela Orsini,* Università di Pisa.
9:40 – 10:10	**Polinomi e Crittografia** *Prof. Michele Elia,* Politecnico di Torino.
10:10 – 10:40	*Coffee break*
10:40 – 11:10	**Algoritmi randomizzati per parole di peso minimo** *Dott.ssa Camilla Ferretti,* Università Cattolica di Piacenza.
11:10 – 11:40	**Funzioni debolmente APN e S-Box a 4 bit** *Dott.ssa Valentina Pulice,* Università di Trento.
11:40 – 12:00	*Coffe break*
12:00 – 12:30	**Presentazione di BunnyTN e prima valutazione di sicurezza** *Dott. Stefano Martin,* Università di Trento.
12:30 – 13:00	**Stream Ciphers e attacchi algebrici** *Dott. Daniele Giovannini*, Università di Trento.
CENA SOCIALE:	*ore 18:30 – Agritur Ponte Alto, Povo (Tn)*

Titoli ed abstract del Workshop di Crittografia "BUNNYTN" – 10 marzo 2011

Sui reticoli ibridi e il crittosistema NTWO

Dott.ssa Emmanuela Orsini, Università di Pisa.

Ore 9:10 – 9:40

Sia i reticoli che i codici a correzione d'errore hanno suscitato nuovo interesse in Crittografia pubblica.
Gli algoritmi computazionalmente difficili in questi ambiti sono difatti ritenuti computazionalmente difficili persino all'interno di modelli computazionali quantistici, mentre gli algoritmi classici cadono in quest'ultimi.
Verranno definiti dei reticoli ibridi che hanno una metrica ad-hoc combinando la metrica Euclidea e quella di Hamming.
Questi reticoli sono costruiti per studiare problemi di correzione dell'errore.
Come risultati saranno mostrati dapprima che il CVP (Closest Vector Problem) nei reticoli ibridi può essere ridotto al CVP in reticoli regolari di dimensione superiore.
Sarà mostrato poi come attaccare col CVP nei reticoli ibridi il crittosistema NTWO, che è simile al più famoso NTRU, ma con l'uso di errori controllati nella creazione della chiave pubblica. Verranno determinati inoltre dei vincoli stringenti sulla dimensione in cui questo attacco può funzionare.

Polinomi e Crittografia

Prof. Michele Elia, Politecnico di Torino.

Ore 9:40 – 10:10

I polinomi occupano da sempre una posizione di rilievo nella matematica, ed in tempi molto recenti il loro impiego è diventato inevitabile nella crittografia. Scopo di questa breve disamina è di rivedere alcune importanti applicazioni di polinomi in crittografia e di illustrare alcune problematiche concernenti sia la loro valutazione sia il calcolo delle loro radici, questioni, peraltro, di grande interesse anche in altre scienze matematiche.
Nella prima parte, verranno brevemente ricordate le seguenti applicazioni crittografiche che mostrano la varietà di uso dei polinomi: 1) trasformazioni non lineari sui campi finiti; 2) trasformazione di Rabin; 3) curve ellittiche nei critto-sistemi in chiave pubblica; 4) schema di secret-sharing proposti da Shamir; 5) trasformazioni nello standard di cifratura a blocchi AES; 6) decrittazione nello schema di McEliece; 7) metodi di distribuzione di chiavi di accesso in sistemi consumer (pay TV); 8) codici correttori d'errore per bio-impronte.
Nella seconda parte, con particolare riferimento agli ultimi tre esempi che coinvolgono polinomi di grado elevato in campi finiti, saranno descritti metodi per:

1) il calcolo delle radici di un polinomio nel campo finito di fattorizzazione completa e con riferimento alla decodifica dei codici algebrici (di lunghezza n); in particolare si delineerà un algoritmo probabilistico di complessità proporzionale a $\sqrt{n}$, anziché ad n come nei metodi standard;
2) la valutazione in un punto di un polinomio di grado m molto elevato; in particolare sarà illustrato un algoritmo che, basato sull'automorfismo di Frobenius, impiega un numero di prodotti asintoticamente proporzionale a $\sqrt{m}$, anziché ad m come nei metodi standard.

Algoritmi randomizzati per parole di peso minimo

Dott.ssa Camilla Ferretti, Università Cattolica di Piacenza.

Ore 10:40 – 11:10

L'intervento affronterà il problema della ricerca di una parola di peso *w* in un codice lineare. Partendo da proposte già esistenti in letteratura si costruisce un *algoritmo randomizzato* che ad ogni iterazione seleziona random un codice equivalente a quello di partenza, finché la parola cercata non appare come somma di un numero piccolo di righe della matrice generatrice. L'algoritmo offre buoni risultati in termini di tempo medio di esecuzione e lascia spazio ad ulteriori miglioramenti per abbassare il costo computazionale. L'algoritmo può essere adottato per attaccare i critto sistemi di tipo McEliece e Niederreiter.

Funzioni debolmente APN e S-Box a 4 bit

Dott.ssa Valentina Pulice, Università di Trento.

Ore 11:10 – 11:40

Partendo da classificazioni note delle S-Box a 4 bit, durante l'intervento si otterranno delle nuove caratterizzazioni per queste funzioni.
In particolare saranno fornite delle condizioni necessarie e/o sufficienti affinché una funzione Booleana vettoriale sia debolmente APN.

Presentazione di BunnyTN e prima valutazione di sicurezza

Dott. Stefano Martin, Università di Trento.

Ore 12:00 – 12:30

Nella prima parte dell'intervento verrà esposta la costruzione del *toy cipher* che si sta sviluppando nel Laboratorio di Crittografia presso il Dipartimento di Matematica dell'Università di Trento: BunnyTN.
Lo scopo di BunnyTN è fornire un esempio di block-cipher abbastanza piccolo per effettuare test approfonditi, ma con costruzione matematica non banale.
Nella seconda parte, mettendosi dal punto di vista del valutatore del sistema, si condurrà una prima analisi di sicurezza di BunnyTN, concentrandosi sulle S-Box e sui test statistici e standard.

Stream Ciphers e attacchi algebrici

Dott. Daniele Giovannini, Università di Trento.

Ore 12:30 – 13:00

Gli stream ciphers sono cifrari a chiave simmetrica che provano ad approssimare il "one-time-pad", dimostrato da Shannon essere impossibile da attaccare se la chiave è perfettamente random.
Nei cifrari a flusso il messaggio criptato si ottiene combinando quello in chiaro con la 'keystream' simbolo a simbolo (ovvero nella maggior parte dei casi tramite una somma bit a bit).
Il problema è generare una 'keystream' che sia più random possibile, che dipenda da una chiave segreta e che non comporti costi computazionali troppo alti.
Saranno presentati tre cifrari di complessità crescente: un 'toy cipher', TRIVIUM e ZUC.
L'intervento si concluderà con una descrizione di alcuni attacchi algebrici sugli stream ciphers.