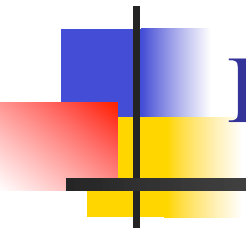
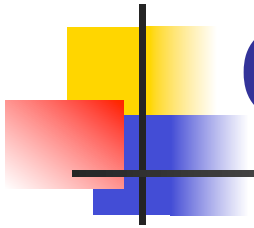


Corso di Crittografia

Prof. Dario Catalano

Cifrari Asimmetrici:

Il cifrario Paillier



Cifrari asimmetrici

- Nella scorsa lezione abbiamo parlato del cifrario El Gamal
  - Cifrario probabilistico, sicuro (contro avversari CPA) relativamente all'ipotesi DH decisionale.
- Adesso studieremo il cifrario Paillier
  - Cifrario omomorfico
- Nelle prossime lezioni guarderemo OAEP
  - Cifrario sicuro contro avversari CCA.
- Prima facciamo un po' di ripasso.

Definizione (ind-cpa)

- AE=(KeyGen, Enc, Dec) cifrario asimmetrico

$Esp_{AE}^{ind\text{-}cpa\text{-}1}(A)$	$Esp_{AE}^{ind\text{-}cpa\text{-}0}(A)$
$(pk,sk) \leftarrow_R KeyGen$	$(pk,sk) \leftarrow_R KeyGen$
$b \leftarrow A^{Enc_{pk}(LR(.,.,1))}$	$b \leftarrow A^{Enc_{pk}(LR(.,.,0))}$
Return b	Return b

$$Adv^{ind\text{-}cpa}(A) = |Pr[Esp_{AE}^{ind\text{-}cpa\text{-}1}(A) = 1] - Pr[Esp_{AE}^{ind\text{-}cpa\text{-}0}(A) = 1]|$$

Definizione (ind-cca)

- AE=(KeyGen, Enc, Dec) cifrario simmetrico

$Esp_{SE}^{ind\text{-}cca\text{-}1}$ (A)	$Esp_{SE}^{ind\text{-}cca\text{-}0}$ (A)
$(pk,sk) \leftarrow_R$ KeyGen	$(pk,sk) \leftarrow_R$ KeyGen
$b \leftarrow A^{Enc_{pk}(LR(.,.,1)),Dec_{sk}(.)}$	$b \leftarrow A^{Enc_{pk}(LR(.,.,0)),Dec_{sk}(.)}$
If A imbroglia Return 0	If A imbroglia Return 0
else return b	else return b

$Adv^{ind\text{-}cca}(A)=|Pr[Esp_{AE}^{ind\text{-}cca\text{-}1}(A)=1] - Pr[Esp_{AE}^{ind\text{-}cca\text{-}0}(A)=1]|$

A imbroglia se interroga $D_k(.)$ su un crittotesto gia' restituito da $Enc_{pk}(LR(.,.,1))$

Introduzione al cifrario Paillier

- Abbiamo visto due tipi di problemi difficili: Logaritmo discreto e varianti di RSA
- Soluzioni basate su RSA possono trarre vantaggio dal fatto che RSA e' una trapdoor perm
- Schemi basati sul logaritmo discreto possono sfruttare la proprieta' omomorfica della funzione esponenziazione.
- Possiamo coniugare i due approcci?

Preliminari Matematici

- Un elemento y in $Z^*_{N^2}$ e' detto N-residuo (mod N^2) se esiste x in $Z^*_{N^2}$ tale che $y=x^N \bmod N^2$

Fatto 1 Ogni N-residuo ammette N radici N-esime distinte.

Fatto 2: Si consideri l'insieme

$$T=\{(1+xN) \bmod N^2 : x \in Z_N\}$$

Ogni elemento $z \in T$ e' tale che $z^N=1 \bmod N^2$.

Fatto 3: L'ordine di $Z^*_{N^2}$ e' $\varphi(N^2)$.

Dunque per ogni x in $Z^*_{N^2}$ si ha che $x^{\varphi(N^2)} \bmod N^2=1$

Osservazioni (sul Fatto 3)

Fatto 3: L'ordine di $Z^*_{N^2}$ e' $\varphi(N^2)$.

- $N=p^2q^2$ ➔ $\varphi(N^2)=(p^2-p)(q^2-q)$
  - Dunque $\varphi(N^2)=\varphi(N)N$
- Ogni N residuo ha ordine $\varphi(N)$.

Il problema della N-residuosita'

- Sia dato un elemento (random) w in $Z^*_{N^2}$, e' w un N residuo oppure no?
- Come vedremo, conoscere la fattorizzazione permette di risolvere in modo efficiente tale problema.

Congettura: Se la fattorizzazione e' ignota non esiste nessun algoritmo (probabilistico) polinomiale per tale problema

Il problema della N residuosita' decisionale

$Esp_N^{DCRA-1}(A)$	$Esp_N^{DCRA-0}(A)$
$x \leftarrow_R Z^*_{N^2}$	$w \leftarrow_R Z^*_{N^2}$
$w \leftarrow x^N \bmod N^2$	$d \leftarrow_R A(w)$
$d \leftarrow_R A(w)$	Return d
Return d	

$$Adv^{DCRA}_N(A)=Pr[Esp^{DCRA-1}_N(A)=1]-Pr[Esp^{DCRA-0}_N(A)=1]$$

Decidere N residuosita'

- Ricordiamo che ogni N residuo ha ordine φ(N).
- Se conosciamo la fattorizzazione, possiamo calcolare φ(N).
- Decidiamo se un dato w e' un N residuo come segue.

N-residuosity(φ(N),w)

if $w^{\varphi(N)}$ return 1

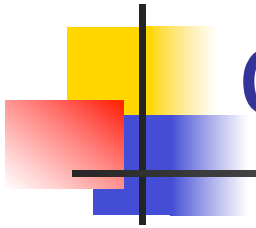
else return 0

Verso lo schema di Paillier

Fatto 4: Ogni elemento $w \in Z^*_{N^2}$ puo' essere scritto nella forma $(1+xN)y^N$, con $x \in Z_N$ e $y \in Z^*_N$.

- Questo fatto suggerisce un'idea interessante.
- Dividiamo $Z^*_{N^2}$ in N classi di equivalenza
  - $a \equiv b$ se ab^{-1} e' un N residuo in $Z^*_{N^2}$.

L'algoritmo di generazione della chiave.



- Molto simile ad RSA.
  - Calcola un modulo N=pq.
  - Ma qui non l'esponente e non ci serve.
- Chiave pubblica: N.
- Chiave privata: la fattorizzazione di N.
- Lo spazio dei messaggi e' Z_N, lo spazio dei crittotesti e' $Z^*_{N^2}$.

L'algoritmo di cifratura

Enc(N, m) // $m \in Z_N$

$y \leftarrow_R Z_N^*$;

$c = (1 + mN)y^N \bmod N^2$

Return c

L'algoritmo di decifratura - I

- E' un po' piu' complicato, descriviamolo passo passo.

Primo passo: Calcoliamo $c^{\varphi(N)}$

$$
\begin{aligned}
c^{\phi(N)} &= \left((1+mN)y^N\right)^{\phi(N)} \bmod N^2 \\
&= (1+mN)^{\phi(N)} y^{N\phi(N)} \bmod N^2 \\
&= (1+mN)^{\phi(N)}
\end{aligned}
$$

L'algoritmo di decifratura - II

Secondo passo.

- Ogni elemento (1+xN) ha ordine N in $Z^*_{N^2}$ (Fatto 2).
- Dunque, poiche' gcd(N, φ(N))=1, esiste d tale che $d\varphi(N)=1 \bmod N$

$$C = \left(c^{\phi(N)}\right)^d = (1+mN)^{\phi(N)d} \bmod N^2$$

$$= (1+mN) \bmod N^2$$

L’algoritmo di decifratura - III

Terzo passo. Calcoliamo m da C come segue

$$m = \frac{C - 1}{N}$$

NB: Si noti che tale calcolo e’ fatto sugli interi

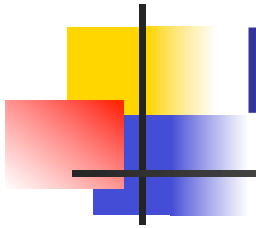
Perche' ci interessa questo cifrario

- Il cifrario di Paillier gode di una proprieta' molto interessante: e' additivamente omomorfico

$$Enc_N(m_1)Enc_N(m_2)=Enc_N(m_1+m_2)$$

- Tale proprieta' e' utilissima in pratica
  - Voto elettronico, Multiparty Computation...

Sicurezza dello schema di Paillier



- Sia N un modulo RSA (fattorizz. ignota)
- A avversario IND-CPA contro lo schema Paillier.
- Esiste B che decide DCRA e tale che

$$Adv_{N,Pai}^{ind\text{-}cpa}(A) \leq 2Adv_{N}^{DCRA}(B)$$

L'avversario B

$\mathbf{B}(N, w)$ // w e' un N residuo?

$(m_0, m_1, \mathtt{st}) \leftarrow A(N)$

$\beta \leftarrow \{0,1\}$;

Sia $c = (1 + m_\beta N)w \bmod N^2$;

$\beta' \leftarrow A(\mathtt{st}, c)$;

if $\beta == \beta'$ return 1

else return 0