

Capitolo 1

Introduzione

Da quando la crittografia ha cessato di essere un'arte per assurgere allo stato di scienza [DH76], sono nati almeno due modi profondamente diversi fra loro di vedere la crittografia.

In uno di questi, il modello *formale*, le operazioni crittografiche sono rappresentate da espressioni simboliche, formali. Nell'altro, il modello *computazionale* le operazioni crittografiche sono viste come funzioni su stringhe di bit e le operazioni hanno una semantica probabilistica. Il primo modello è stato ampiamente trattato in [AG99, BAN90, Kem87, Pau98]. Il secondo modello trova le basi in lavori di altrettanto illustri studiosi .

Il modello formale fino ad oggi è stato sicuramente trattato in modo più approfondito. Questo ha fatto sì che lo stato dell'arte veda molti più tool di verifica automatica che lavorano nel modello formale rispetto a tool che lavorano nel modello crittografico. Uno fra i più famosi tool che lavora nel modello formale è sicuramente il *ProVerif*¹. I sostenitori del modello formale affermano che è molto conveniente ignorare i dettagli di una funzione crittografica e lavorare invece con una descrizione più di alto livello di questa che non includa dettagli riguardanti la funzione crittografica. I sostenitori del modello crittografico computazionale invece affermano che la visione del modello formale non è molto realistica e che le funzioni crittografiche non devono essere viste come espressioni formali ma come algoritmi probabilistici. Inoltre i sostenitori del modello formale, trattando le primitive crittografiche come dei simboli impenetrabili, assumono implicitamente che siano corrette e inviolabili, cosa non esatta. D'altra parte il modello formale ha molti vantaggi come quello precedentemente accennato che riguarda la semplicità con cui vengono costruiti strumenti automatici per la verifica di protocolli in questo modello. Sembrerebbe quindi che esista un divario molto ampio fra

¹Per informazioni più dettagliate su questo tool si visiti il seguente sito web: <http://www.proverif.ens.fr/>

i due modelli. In effetti così è, ma non sono mancati i tentativi di unificare i due modelli, o comunque di cercare una linea di collegamento che li congiunga. In [AR07] gli autori cercano per la prima volta di porre le basi per iniziare a collegare questi due modelli. In particolare il principale risultato di questo lavoro afferma che: se due espressioni nel modello formale sono equivalenti, una volta dotate di un'opportuna semantica probabilistica, vengono mappati in *ensemble* computazionalmente indistinguibili; quindi, sotto forti ma accettabili ipotesi², l'equivalenza formale implica l'indistinguibilità computazionale. È quindi lecito affermare che un attaccante per il modello computazionale non è più potente di un attaccante nel modello formale. Questo risultato ha dato un'ulteriore spinta ai sostenitori del modello formale che potevano così dimostrare risultati nel modello formale, con tutti i benefici che questo portava, e estendere questo risultato al modello computazionale senza troppi problemi. Un'altra strada, invece, è quella che prevede di lavorare direttamente nel modello computazionale senza magari preoccuparsi di rispettare forti ipotesi che erano state usate per dimostrare quel risultato.

il concetto di sicurezza perfetta e quella computazionale per poi riprendere quest'ultima nel capitolo 1 parlare di sicurezza TEORICA vs COMPUTAZIONALE parlare delle assunzioni....e delle funzioni one-way tecnica riduzionista.

²Un'importante ipotesi usata nella dimostrazione del risultato in questione è che non devono esserci crittografici, ovvero si considerano solo schemi crittografici in cui una chiave k , non è mai *cifrata* attraverso k stessa.

Capitolo 2

Il Modello Computazionale

In questo capitolo si cercherà di descrivere le principali caratteristiche del modello computazionale. Saranno resi evidenti alcuni legami che esistono fra la crittografia, la teoria della calcolabilità e alcune nozioni di statistica e probabilità. Sono questi infatti i cardini su cui poggia la crittografia computazionale.

Si cercherà sempre di dare delle definizioni rigorose e il più possibile non ambigue. Si tenterà sempre, inoltre, di fornire delle dimostrazioni delle affermazioni che si fanno; è questo infatti il giusto modo di procedere. Non è raro infatti, trovare esempi di schemi crittografici che sono stati ritenuti validi solo sulla base di argomentazioni approssimative e non formali e che non essendo stati dimostrati *matematicamente* validi si sono poi rivelati tutt'altro che affidabili¹.

2.1 L'Avversario

Il tipico avversario con cui si ha a che fare quando si studiano cifrari o protocolli crittografici nel modello computazionale, è un avversario con risorse di calcolo *limitate*. Limitate nel senso che si sceglie di porre un limite alla potenza di calcolo dell'avversario. Questo significa che non avremo a che fare con un avversario che ha una capacità di calcolo potenzialmente infinita o un tempo illimitato a disposizione.

Sebbene siano stati ideati cifrari sicuri anche rispetto ad avversari non limitati², questi hanno alcuni difetti come per esempio il fatto che la chiave debba

¹Il cifrario di Vigenère ritenuto indecifrabile per moltissimi anni si può infatti violare facilmente con tecniche di tipo statistico.

²Il cifrario *one-time pad* è il tipico esempio di cifrario perfettamente sicuro o teoricamente sicuro.

essere lunga quanto il messaggio o che sia utilizzabile una sola volta. Per rappresentare in modo formale un avversario con risorse di calcolo limitate, si può rappresentare questo come un generico algoritmo appartenente ad una particolare classe di complessità computazionale³.

Una linea di pensiero che accomuna ogni campo dell'informatica, considera efficienti gli algoritmi che terminano in un numero di passi polinomiale nella lunghezza dell'input, e inefficienti quelli che hanno una complessità computazionale maggiore (e.g. esponenziale). La scelta di porre un limite alle risorse di calcolo dell'avversario è dettata dal buon senso. È ragionevole infatti pensare che l'attaccante non sia infinitamente potente; è altrettanto ragionevole pensare che un attaccante non sia disposto ad impiegare un tempo *eccessivo* per violare uno schema crittografico.

È logico quindi pensare che gli avversari vogliano essere *efficienti*.

Può sembrare quindi naturale immaginare gli avversari come degli algoritmi che terminano in un numero polinomiale di passi rispetto alla lunghezza dell'input. Come si può notare, non si fa alcuna assunzione particolare sul comportamento dell'avversario. Le uniche cose che sappiamo sono che:

- l'avversario non conosce la chiave, ma conosce l'algoritmo di cifratura utilizzato e i parametri di sicurezza, come per esempio la lunghezza della chiave⁴.
- l'avversario vuole essere efficiente, ovvero polinomiale.

Non si fanno ipotesi sull'algoritmo che questo andrà ad eseguire. Per esempio dato un messaggio cifrato $c = E_k(m)$, non ci aspettiamo che l'avversario non decida di utilizzare la stringa c' tale che: $c' = D_{k'}(E_k(m))$ con $k \neq k'$. Ovvero, sarebbe sbagliato supporre che l'avversario non cerchi di decifrare un messaggio mediante una chiave diversa da quella utilizzata per cifrarlo. Nel modello computazionale i messaggi sono trattati come sequenze di bit e non come espressioni *formali*; l'avversario, nel modello computazionale, può effettuare qualsiasi operazione su un messaggio. Questa visione è, a differenza di quella che si ha nel modello formale, sicuramente molto più realistica [Dwo06].

Non bisogna però dimenticare che un avversario può sempre *indovinare* il segreto che cerchiamo di nascondere o che cifriamo. Per esempio: se il segreto che si cerca di nascondere ha una lunghezza di n bit, l'avversario può sempre

³Un avversario infatti è una macchina di Turing che esegue un algoritmo.

⁴Il principio di Kerchoffs (famoso crittografo olandese, 19 Gennaio 1835 - 9 Agosto 1903) afferma che l'algoritmo di cifratura non deve essere segreto e deve poter cadere nelle mani del nemico senza inconvenienti.

effettuare una scelta casuale fra il valore 0 e il valore 1 per n volte. La probabilità che l'avversario ottenga una stringa uguale al segreto è ovviamente di $\frac{1}{2^n}$. Questa probabilità tende a 0 in modo esponenziale al crescere della lunghezza del segreto, ma per valori finiti di n questa probabilità non sarà mai 0. È quindi più realistico cercare di rappresentare l'avversario come un algoritmo che, oltre a terminare in tempo polinomiale, ha anche la possibilità di effettuare scelte casuali e di commettere errori (anche se con probabilità limitata). La classe dei problemi risolti da questo tipo di algoritmi è indicata con la sigla *BPP* (i.e. *Bounded-Probability Polynomial Time*).

Un modo più formale di vedere questo tipo di algoritmi è il seguente: si suppone che la macchina di Turing che esegue l'algoritmo, oltre a ricevere l'input, diciamo x , riceva anche un input ausiliario r . Questa stringa di bit r , rappresenta una possibile sequenza di lanci di moneta dove è stato associato al valore 0 la croce e al valore 1 la testa (o anche viceversa ovviamente). Quando la macchina dovesse effettuare una scelta casuale, non dovrà far altro che prendere il successivo bit dalla stringa r , e prendere una decisione in base ad esso (è, in effetti, come se avesse preso una decisione lanciando una moneta). Ecco quindi che il nostro tipico avversario si configura come un algoritmo polinomiale probabilistico. È inoltre giustificato cercare di rendere sicuri⁵ gli schemi crittografici rispetto, principalmente, a questo tipo di avversario. Non è quindi necessario dimostrare che un particolare schema crittografico sia inviolabile, ma basta dimostrare che:

- in tempi ragionevoli lo si può violare solo con scarsissima probabilità.
- lo si può violare con alta probabilità, ma solo in tempi non ragionevoli.

Sappiamo che il concetto di *tempo ragionevole* è catturato dalla classe degli algoritmi polinomiali probabilistici. Vediamo ora di catturare il concetto di *scarsa probabilità*.

2.2 Funzioni Trascurabili e non ...

In crittografia i concetti di *scarsa probabilità* e di evento *raro* vengono formalizzati attraverso la nozione di funzione trascurabile.

Definizione 2.1 *Funzione Trascurabile.* Sia $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ una funzione. Si dice che μ è trascurabile se e solo se per ogni polinomio p , esiste $C \in \mathbb{N}$ tale che $\forall n > C: \mu(n) < \frac{1}{p(n)}$.

⁵In qualsiasi modo si possa intendere il concetto di sicurezza. Vedremo che in seguito si daranno delle definizioni rigorose di questo concetto.

Una funzione trascurabile, quindi, è una funzione che tende a 0 più velocemente dell'inverso di qualsiasi polinomio. Un'altra definizione utile è la seguente:

Definizione 2.2 *Funzione Distinguibile.* Sia $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ una funzione. Si dice che μ è distinguibile se e solo se esiste un polinomio p , tale per cui esiste $C \in \mathbb{N}$ tale che $\forall n > C: \mu(n) > \frac{1}{p(n)}$.

Per esempio la funzione $n \mapsto 2^{-\sqrt{n}}$ è una funzione trascurabile, mentre la funzione $n \mapsto \frac{1}{n^2}$ non lo è. Ovviamente esistono anche funzioni che non sono né trascurabili né distinguibili. Per esempio, la seguente funzione definita per casi:

$$f(n) = \begin{cases} 1, & \text{se } n \text{ è pari} \\ 0, & \text{se } n \text{ è dispari} \end{cases}$$

non è né trascurabile né distinguibile. Questo perché le definizioni precedenti, pur essendo molto legate, non sono l'una la negazione dell'altra.

Se sappiamo che, in un esperimento, un evento avviene con una probabilità trascurabile, quest'evento si verificherà con una probabilità trascurabile anche se l'esperimento viene ripetuto molte volte (ma sempre un numero polinomiale di volte), e quindi per la legge dei grandi numeri, con una frequenza anch'essa trascurabile⁶. Le funzioni trascurabili, infatti, godono di due particolari proprietà di chiusura, enunciate nella seguente:

Proposizione 2.1 *Siano μ_1, μ_2 due funzioni trascurabili e sia p un polinomio. Se $\mu_3 = \mu_1 + \mu_2$, e $\mu_4 = p \cdot \mu_1$, allora μ_3, μ_4 sono funzioni trascurabili.*

Se quindi, in un esperimento, un evento avviene solo con probabilità trascurabile, ci aspettiamo che, anche se ripetiamo l'esperimento un numero polinomiale di volte, questa probabilità rimanga comunque trascurabile. Per esempio: supponiamo di avere un dado truccato in modo che la probabilità di ottenere 1 sia trascurabile. Allora se lanciamo il dado un numero polinomiale di volte, la probabilità che esca 1 rimane comunque trascurabile. È ora importantissimo notare che: **gli eventi che avvengono con una probabilità trascurabile possono essere ignorati per fini pratici.** In [KL07], infatti leggiamo:

Events that occur with negligible probability are so unlikely to occur that can be ignored for all practical purposes. Therefore, a break of a cryptographic scheme that occurs with negligible probability is not significant.

⁶In modo informale, la legge debole dei grandi numeri afferma che: per un numero grande di prove, la frequenza approssima la probabilità di un evento.

Potrebbe sembrare pericoloso utilizzare degli schemi crittografici che ammettono di essere violati con probabilità trascurabile, ma questa possibilità è così remota, che una tale preoccupazione è da ritenersi ingiustificata. Finora abbiamo parlato di funzioni che prendono in input un argomento non meglio specificato. Al crescere di questo parametro, le funzioni si comportano in modo diverso, a seconda che siano trascurabili, oppure no. Ma cosa rappresenta nella realtà questo input? Di solito, questo valore rappresenta un generico parametro di sicurezza, indipendente dal segreto. È comune immaginarlo come la lunghezza in bit delle chiavi.

D'ora in poi con affermazioni del tipo «l'algoritmo è polinomiale, o esponenziale», si intenderanno algoritmi polinomiali o esponenziali nella lunghezza (in bit) del parametro di sicurezza (indicato con n). Si utilizzerà questa assunzione anche quando si faranno affermazioni su funzioni trascurabili o meno. Quelle funzioni saranno trascurabili o meno nel parametro n . Tutte le definizioni di sicurezza che vengono date nel modello computazionale e che utilizzano le probabilità trascurabili, sono di tipo *asintotico*. Un template di definizione di sicurezza è il seguente [KL07]:

A scheme is secure if for every probabilistic polynomial-time adversary \mathbf{A} [...], the probability that \mathbf{A} succeeds in this attack [...] is negligible

Essendo questo schema di definizione asintotico (nel parametro di sicurezza n), è ovvio che non considera valori piccoli di n . Quindi se si dimostra che un particolare schema crittografico è sicuro secondo una definizione di questo tipo, può benissimo capitare che per valori piccoli di n lo schema sia violabile con alta probabilità e in tempi ragionevoli.

2.3 Indistinguibilità Computazionale

Se due oggetti, sebbene profondamente diversi fra loro, non possono essere distinti, allora sono, da un certo punto di vista, equivalenti. Nel caso della crittografia computazionale, due oggetti sono computazionalmente equivalenti se nessun algoritmo efficiente li può distinguere. Possiamo immaginare che un algoritmo riesca a distinguere due oggetti, se quando gli si dà in input il primo, lui dà in output una costante c , mentre se gli si fornisce come input il secondo dà in output una costante c' e ovviamente $c \neq c'$. La definizione tipica di indistinguibilità computazionale è data prendendo come oggetti da distinguere alcune particolari distribuzioni statistiche detti *ensembles*.

Definizione 2.3 *Ensemble.* Sia I un insieme numerabile infinito. $X = \{X_i\}_{i \in I}$ è un ensemble su I se e solo se è una sequenza di variabili statistiche, tutte con lo stesso tipo di distribuzione.

Un *ensemble* è quindi una sequenza infinita di distribuzioni di probabilità⁷. Tipicamente le variabili dell'ensemble sono stringhe di lunghezza i . X_i è quindi una distribuzione di probabilità su stringhe di lunghezza i .

Ora supponiamo di avere due ensemble X e Y . Intuitivamente queste distribuzioni sono indistinguibili se nessun algoritmo (efficiente) può accettare infiniti elementi di X_n (per esempio stampando 1 su input preso da X_n) e scartare infiniti elementi di Y_n (per esempio stampare 0 su input preso da Y_n). È importante notare che sarebbe facile distinguere due *singole* distribuzioni usando un approccio esaustivo, ecco perché si considerano sequenze infinite di distribuzioni finite. In poche parole questi ensemble sono indistinguibili se ogni algoritmo (efficiente) accetta $x \in X_n$ se e solo se accetta $y \in Y_n$. Ovviamente il *se e solo se* non può e non deve essere inteso in senso *classico*, ma deve essere inteso in senso statistico. Poiché in crittografia si è soliti indicare con U_m una variabile uniformemente distribuita sull'insieme delle stringhe di lunghezza m , chiameremo $U = \{U_n\}_{n \in \mathbb{N}}$ l'ensemble uniforme. Dopo questa breve introduzione all'indistinguibilità siamo pronti per dare una definizione rigorosa:

Definizione 2.4 *Indistinguibilità computazionale.* Due ensemble $X = \{X_n\}$, $Y = \{Y_n\}$ sono computazionalmente indistinguibili se e solo se per ogni algoritmo $D \in BPP$ (detto *distinguitore*) esiste μ trascurabile tale che:

$$|Pr[D(1^n, X_n) = 1] - Pr[D(1^n, Y_n) = 1]| \leq \mu(n).$$

Nella definizione precedente: $Pr[D(1^n, X_n) = 1]$ è la probabilità che, scegliendo x secondo la distribuzione X_n e fornendo questo valore al distinguitore insieme al valore 1^n , il distinguitore stampi 1. Il fatto che al distinguitore si fornisca anche il valore del parametro di sicurezza in base unaria, serve ad esser sicuri che in ogni caso il distinguitore impieghi un tempo polinomiale nel parametro di sicurezza. Infatti, il distinguitore quando si troverà a dover leggere il primo parametro, necessariamente impiegherà un tempo polinomiale nel parametro di sicurezza, visto che questo è stato fornito in base unaria⁸.

⁷Siccome si parla di distribuzioni su stringhe di bit con lunghezza finita, in crittografia computazionale si considerano ensemble che sono una sequenza infinita di distribuzioni finite di stringhe di bit.

⁸Ignoreremo, d'ora in poi, questo cavillo formale.

La definizione di indistinguibilità computazionale cattura quindi il seguente concetto: se due ensemble sono computazionalmente indistinguibili, allora la probabilità che un distinguitore riesca a discernere i valori provenienti da un insieme rispetto all'altro è trascurabile; di conseguenza agli occhi del distinguitore gli ensemble non sono differenti e quindi sono per lui equivalenti (o meglio computazionalmente equivalenti o ancora, indistinguibili in tempo polinomiale). Non è raro, nell'ambito scientifico in particolare, basarsi sul concetto generale di indistinguibilità al fine di creare nuove classi di equivalenza di oggetti.

The concept of efficient computation leads naturally to a new kind of equivalence between objects: Objects are considered to be computationally equivalent if they cannot be differentiated by any efficient procedure. We note that considering indistinguishable objects as equivalent is one of the basics paradigms of both science and real-life situations. Hence, we believe that the notion of computational indistinguishability is a very natural one [Gol00].

2.4 Pseudocasualità e Generatori Pseudocasuali

Argomento centrale di questa sezione è il concetto di *pseudocasualità* applicato a stringhe di bit di lunghezza finita. Parlare di pseudocasualità applicata ad una *singola* stringa, ha poco senso quanto ne ha poco parlare di singola stringa casuale. Il concetto di casualità (come quello di pseudocasualità) si applica, infatti, a distribuzioni di oggetti (stringhe di bit nel nostro caso) e non a singoli oggetti.

La nozione di casualità è fortemente legata a quella di distribuzione uniforme. Un insieme di oggetti è caratterizzato da una distribuzione uniforme se la probabilità è equamente distribuita su tutti gli oggetti. Quindi *l'estrazione* di un elemento è del tutto casuale, perché non ci sono elementi più probabili di altri.

Il concetto di pseudocasualità è un caso particolare di indistinguibilità, infatti una distribuzione è *pseudocasuale* se nessuna procedura efficiente, può distinguerla dalla distribuzione uniforme.

Definizione 2.5 *Pseudocasualità.* L'ensemble $X = \{X_n\}_{n \in \mathbb{N}}$ è detto *pseudocasuale* se e solo se $\exists l : \mathbb{N} \rightarrow \mathbb{N}$ tale che: X è computazionalmente indistinguibile da $U = \{U_{l(n)}\}_{n \in \mathbb{N}}$.

Data questa definizione, possiamo finalmente definire formalmente cosa sia un generatore pseudocasuale.

Definizione 2.6 *Generatore Pseudocasuale.* Sia $l : \mathbb{N} \rightarrow \mathbb{N}$ un polinomio detto fattore d'espansione. Sia G un algoritmo polinomiale deterministico tale che: $\forall s \in \{0, 1\}^n G(s) \in \{0, 1\}^{l(n)}$. Allora G è un generatore pseudocasuale se e solo se valgono le seguenti condizioni:

- *Espansione:* $\forall n : l(n) > n$
- *Pseudocasualità:* $\forall D \in BPP, \exists \mu$ trascurabile tale che

$$|Pr[D(r) = 1] - Pr[D(G(s)) = 1]|$$

con $r \in U_{l(n)}$ e $s \in U_n$

Quindi: se data una stringa di bit $s \in U_n$, nessun distinguitore efficiente riesce a distinguere (con una probabilità non trascurabile) $G(s)$ da una stringa $r \in U_{l(n)}$, allora G è un generatore pseudocasuale. Il suo output, infatti, non è distinguibile dalla distribuzione effettivamente uniforme.

È importante però notare, che la distribuzione di stringhe in output di un generatore pseudocasuale è fortemente differente dalla distribuzione effettivamente casuale. Per rendere più chiara questa distinzione procederemo con un importante esempio. Supponiamo di avere un generatore pseudocasuale G con fattore d'espansione $l(n) = 2n$. L'insieme $A = \{0, 1\}^{2n}$ ha, ovviamente, una cardinalità pari a 2^{2n} . Fissando quindi una certa stringa $x \in A$, questa ha una probabilità di esser scelta in maniera casuale pari a: $\frac{1}{|A|} = \frac{1}{2^{2n}}$.

Ragioniamo adesso sull'output del generatore G . Questo prende un input appartenente al dominio: $B = \{0, 1\}^n$. Anche considerando il caso *migliore* di un generatore iniettivo⁹, il codominio di G avrà una cardinalità pari a quella del dominio ovvero 2^n . La maggior parte degli elementi dell'insieme A non ricadrà nell'output di G ; questo a causa dell'abissale differenza di cardinalità fra gli insiemi $G(B)$ e A . Quindi la probabilità che una stringa scelta in maniera uniforme dall'insieme A ricada nel codominio di G è di $\frac{2^n}{2^{2n}}$, cioè 2^{-n} . In teoria, quindi, è facile immaginare un distinguitore D che riesca a discernere l'output di G dalla distribuzione uniforme con probabilità non trascurabile. Supponiamo che D prenda in input $y \in A$. Tutto ciò che D deve fare è ricercare in modo esaustivo un $w \in B$ tale che $G(w) = y$. Se $y \in G(B)$ allora D se ne accorgerà con probabilità 1, mentre se y è stato scelto in maniera uniforme dall'insieme A , D stamperà 1 con probabilità 2^{-n} .

⁹Una generica funzione f è iniettiva se e solo se $\forall x_1, x_2 : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Quindi abbiamo che:

$$|Pr[D(r) = 1] - Pr[D(G(s)) = 1]| \geq 1 - 2^{-n}$$

con $r \xleftarrow{R} A$ e $s \xleftarrow{R} B$ ¹⁰.

Il membro a destra della disequazione è una funzione distinguibile. Sembra quindi che G non sia un generatore pseudocasuale. C'è un'importante constatazione da fare però. Il distinguitore D non è efficiente! Infatti impiega un tempo esponenziale nel parametro n , e non polinomiale. La distribuzione generata da G dunque, è sì ben lontana dall'essere uniforme, ma questo non è importante dal momento che nessun distinguitore che viaggia in tempo polinomiale può accorgersene.

Nella pratica lo scopo di G è prendere in input un *seed* casuale, e da quello generare una variabile pseudocasuale molto più lunga. Si intuisce da questo la grandissima importanza che hanno i generatori pseudocasuali in crittografia. Per esempio il seed potrebbe corrispondere alla chiave di un cifrario, mentre l'output di G di lunghezza k potrebbe essere il valore con cui viene fatto lo *XOR* del messaggio (anch'esso di lunghezza k); otteniamo così una versione del one-time pad basato su una chiave più corta del messaggio. Siccome una stringa pseudocasuale appare, ad un distinguitore efficiente D , come una stringa casuale, D non ottiene un vantaggio sensibile nel passaggio dal vero one-time pad al one-time pad che usa una chiave pseudocasuale. In generale i generatori pseudocasuali sono molto utili in crittografia per creare schemi crittografici simmetrici.

2.5 Dimostrazioni Basate su Games

In questo paragrafo si cercherà di spiegare cosa siano nell'ambito della crittografia i *games*¹¹ e come siano strutturate la maggior parte delle dimostrazioni che utilizzano sequenze di games.

Si possono trovare approfondimenti riguardo a questi concetti nel lavoro di Shoup [Sho]. Quella basata sul concetto di game è una tecnica¹² molto utilizzata per provare la sicurezza di primitive crittografiche o di protocolli crittografici. Questi games sono giocati da un'ipotetica entità maligna, l'attaccante, e da un'ipotetica parte benigna di solito chiamato sfidante¹³. È difficile dare una definizione formale di game; infatti il concetto di game

¹⁰Con la notazione $s \xleftarrow{R} O$, si intende la scelta dell'elemento $s \in O$ in maniera casuale.

¹¹Che intenderemo letteralmente come giochi.

¹²Game hopping technique.

¹³Perché *sfida* l'attaccante a vincere questo gioco.

cambia, sebbene in maniera non sensibile, da situazione a situazione, da ambiente ad ambiente e da dimostrazione a dimostrazione (sia che queste siano fatte manualmente sia che queste siano automatiche e quindi dipendenti dal framework in cui vengono costruite). Intuitivamente però, i game possono essere immaginati come un insieme di azioni, modellate in una particolare algebra di processi, che servono a specificare il comportamento dei partecipanti al gioco, ovvero le entità che partecipano come *principals* al protocollo crittografico.

Il lettore troverà utile pensarli, almeno nell'ambito di questa tesi, come insiemi di processi che, fra le altre cose, forniscono un'interfaccia all'attaccante attraverso degli *oracoli* che possono restituire dei valori all'attaccante. Questi oracoli, prima di ritornare il valore, possono effettuare calcoli, dichiarare ed utilizzare variabili che non saranno visibili all'esterno.

Si deve pensare agli oracoli come delle scatole nere inaccessibili dall'esterno. Questi oracoli una volta interrogati forniscono una risposta, e questo è il massimo livello di interazione che dall'esterno si può avere con queste entità.

Il primo passo che le dimostrazioni di sicurezza basate su sequenze di game fanno, è quello di modellare il protocollo crittografico reale in un game iniziale G_0 . In G_0 esiste la probabilità non nulla che un evento *negativo* possa accadere (immaginiamolo come una sorta di vittoria da parte dell'attaccante). Ora, in generale, si procede effettuando delle modifiche al game G_i ottenendo un game G_{i+1} tale che G_i e G_{i+1} siano computazionalmente indistinguibili. Le modifiche che si effettuano fra un game e un altro devono introdurre delle differenze computazionalmente irrilevanti. Queste modifiche possono essere viste come regole di riscrittura delle distribuzioni di probabilità delle variabili in gioco nei game. Se per esempio in un game G_i un processo ha a che fare con un variabile casuale, e nel game G_{i+1} questa viene sostituita con una variabile che invece è pseudocasuale, non vengono introdotte modifiche computazionalmente rilevanti e quindi il passaggio è lecito, visto che i due game non sono distinguibili se non con probabilità trascurabile. Alla fine si arriva ad un game G_f in cui l'evento non può accadere. Se, quindi, nel game finale l'attaccante non ha possibilità di vincere e il game finale è computazionalmente indistinguibile dal penultimo, questo lo è dal terzultimo e così via fino a G_0 , allora il game finale è computazionalmente indistinguibile dal primo¹⁴. Adesso, quindi, se nel game iniziale esiste la possibilità che un evento avvenga, e nel game finale no, si può dare un limite superiore alla probabilità che l'evento avvenga nel game iniziale. Questo limite è la somma di tutte le probabilità con cui un attaccante riesce a distinguere un game dal

¹⁴Ricordiamo infatti che la somma di due probabilità trascurabili rimane trascurabile.

successivo all'interno della sequenza.

È importante dire che, anche nel modello formale si possono utilizzare le sequenze di game, la differenza è che due game successivi non sono computazionalmente indistinguibili ma sono perfettamente indistinguibili. In particolare quello che si vuole sottolineare è che: se in una sequenza di game G_b e G_a sono l'uno il successore dell'altro, allora i due game devono appartenere ad una stessa classe di equivalenza indotta dalla particolare relazione di equivalenza che il modello in cui si sta costruendo la catena di games sfrutta. Nel modello formale questa relazione sarà l'indistinguibilità perfetta (meglio nota come equivalenza osservazionale) mentre in quello computazionale sarà l'indistinguibilità computazionale.

Capitolo 3

CryptoVerif

CryptoVerif è un *dimostratore* automatico che lavora direttamente nel modello computazionale. È un tool molto recente e in continuo sviluppo.

CryptoVerif è stato scritto da Bruno Blanchet¹ in ML. Si possono trovare più informazioni nella home page di Blanchet². Questo tool è utilizzato per dimostrare proprietà di segretezza e autenticazione. Queste prove si basano sulla tecnica delle sequenze di game. Il tool è liberamente scaricabile³ sotto la licenza CeCill⁴. CryptoVerif è stato già utilizzato per dimostrare la correttezza di alcuni protocolli crittografici, come per esempio: FDH [BP06], Kerberos [BJST08].

3.1 Un Esempio: FDH

Full Domain Hash è uno schema di firma che segue il paradigma *hash-and-sign*⁵. Quella che a breve seguirà è una sequenza di game costruita dal CryptoVerif che dà un limite superiore alla probabilità che un attaccante riesca a forgiare una firma valida per un messaggio. L'input che si fornisce al CryptoVerif consta di un game iniziale chiamato G_0 in cui si modella la sicurezza dello schema e delle equivalenze necessarie a CryptoVerif per effettuare le modifiche ai game. La descrizione dello schema di firma *FDH* viene data al CryptoVerif attraverso il seguente game:

¹Ricercatore al LIENS (Computer Science Laboratory of Ecole Normale Supérieure)

²<http://www.di.ens.fr/~blanchet/index-eng.html>

³<http://www.cryptoverif.ens.fr/cryptoverif.html>

⁴<http://www.cecill.info/licences/>

⁵Questo paradigma vuole che: dato un messaggio m se ne ritorni la firma di $hash(m)$ e non la firma di m , dove la funzione hash può essere istanziata con qualsiasi funzione hash collision resistant. Si ottiene così una firma di lunghezza fissa e non dipendente dalla lunghezza del messaggio

```

 $G_0$ equiv foreach iH ≤ qH do OH(x: bitstring):= return(hash(x)); |

Ogen():=r  $\xleftarrow{R}$  seed;pk ← pkgen(r);sk ← skgen(r);return(pk);
(foreach iS ≤ qS do OS(m: bitstring):= return(invf(sk, hash(m))); |

find u ≤ qS suchthat (defined(m[u]) ∧ m' = m[u])) then end
else event forge

```

Possiamo vedere come in questo game si forniscano qH copie dell' oracolo OH i quali ritornano l'hash della stringa che gli si fornisce in input ovvero x . Abbiamo poi il processo $Ogen()$ che ritorna al contesto una chiave pubblica dopo aver creato, partendo da un seme casuale, una coppia costituita da una chiave privata e una chiave pubblica. Abbiamo poi qS copie dell'oracolo OS che si occupano di fornire una firma del messaggio che gli viene dato in input. Infine abbiamo un singolo oracolo OT che si occupa di verificare se la firma s è valida per il messaggio m' . In particolare se $hash(m') \neq f(pk, s)$ allora la firma non è valida per il messaggio. Se invece $hash(m') = f(pk, s)$ l'oracolo si occupa di verificare se, per il messaggio m' , è stata mai rilasciata una firma dall'oracolo OS , in caso affermativo il processo termina, altrimenti significa che il contesto, ovvero l'attaccante, è stato in grado di forgiare una firma valida per il messaggio, e quindi è avvenuto l'evento *forge*. Notiamo come l'attaccante non sia modellato esplicitamente, infatti non possiamo fare nessuna assunzione sul comportamento di questo. Possiamo immaginare un attaccante come un altro processo non meglio specificato messo in parallelo con questo game. In gergo l'attaccante viene anche detto anche *contesto*. Per poter trasformare un game in un altro CryptoVerif ha bisogno di alcune equivalenze da poter utilizzare. Le definizioni in CryptoVerif vengono fornite attraverso delle equivalenze che possono essere viste come regole di riscrittura delle distribuzioni di probabilità delle variabili in gioco. Queste regole di riscrittura di un generico elemento L in un generico elemento R possono valere incondizionatamente, oppure possono valere a meno di una certa probabilità. Nel secondo caso la riscrittura di un termine L nell'equivalente R comporta l'introduzione di una differenza non nulla fra i due game.

Prima di descrivere il secondo input di CryptoVerif è necessario fare una piccola digressione riguardo al concetto di funzione *one-way*. Intuitivamente una funzione f è one-way se non può essere invertita facilmente. Cioè se dato $y = f(x)$ è arduo riuscire a trovare un x' tale che $f(x') = y$. Si noti come non sia necessario, per invertire la funzione, trovare x ma è sufficiente trovare un x' qualsiasi tale che $f(x') = y$.

Possiamo ora dare la seguente:

Definizione 3.1 *Funzione One-Way.* $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ è *one-way* se e solo se $\forall x \in \{0, 1\}^*, \forall A \in PPT: |Pr[A(f(x)) \in f^{-1}(f(x))]|$ è una funzione trascurabile.

È importante notare come la definizione valga per ogni x del dominio; con questo si vuole sottolineare che invertire f deve essere *sempre* difficile e non per particolari x . È importante affermare ciò perchè tutta la crittografia moderna è fondata sull'ipotesi che esistano le funzioni one-way. Si parla di ipotesi perchè, sebbene la maggior parte degli informatici ne sia convinta, non è stato ancora dimostrata l'esistenza di funzioni di questo genere⁶. La dimostrazione dell'esistenza di funzioni one-way comporterebbe, tra l'altro, anche la risoluzione della famosa questione riguardo agli insiemi P e NP ⁷. Il fatto che però qualcuno un giorno possa dimostrare che $P \neq NP$ non dimostrerebbe affatto l'esistenza delle funzioni one-way. Infatti una funzione one-way deve, come prima sottolineato, essere non invertibile in modo efficiente, sempre e non solo nel *caso pessimo*.

⁶Questo non toglie che esistono funzioni che si avvicinano all'idea che abbiamo di funzioni one-way, per esempio SHA1, o MD5.

⁷ P è l'insieme dei problemi risolvibili nel caso pessimo in un numero di passi polinomiale nell'input. NP invece, è l'insieme dei problemi per cui dato un certo valore, si può verificare in tempo polinomiale se questo è o meno soluzione del problema (ovvero è l'insieme dei problemi con certificazione polinomiale.). Non è ancora noto se questi insiemi siano o meno lo stesso insieme.

Siamo ora pronti per vedere come il concetto di funzione one-way viene modellato in CryptoVerif.

Si tratta di dare una definizione di one-way per mezzo di un'equivalenza fra games. La definizione è la seguente:

equiv

foreach $ik \leq nk$ **do** $r \xleftarrow{R} \text{seed}$; ($\text{Opk}() := \text{return}(r)$;) |

foreach $iF \leq nF$ **do** $x \xleftarrow{R} D$; ($\text{Oy}() := \text{return}(f(\text{pkgen}(r), x))$; |

foreach $i1 \leq n1$ **do** $\text{Oeq}(x': D) := \text{return}(x'=x)$; |

$\text{Ox}() := \text{return}(x)$;

\approx_{pow}

foreach $ik \leq nk$ **do** $r \xleftarrow{R} \text{seed}$; ($\text{Opk}() := \text{return}(r)$;) |

foreach $iF \leq nF$ **do** $x \xleftarrow{R} D$; ($\text{Oy}() := \text{return}(f'(\text{pkgen}'(r), x))$; |

foreach $i1 \leq n1$ **do** $\text{Oeq}(x': D) := \text{if defined}(k) \text{ then return}(x'=x)$;
else return}(false); |

$\text{Ox}() := k \leftarrow \text{mark}; \text{return}(x)$;

Questa equivalenza cattura e definisce il concetto di funzione one-way. La funzione f , infatti, è one-way se e solo se vale l'equivalenza $nNXXX$. Supponiamo che la funzione f non sia one-way, esisterà dunque un avversario efficiente A che riuscirà ad invertire la funzione. A sarà dunque in grado di distinguere i due membri dell'equivalenza $L \approx_{pow} R$. Infatti l'avversario non dovrà far altro che chiamare $\text{Oy}()$, e invertire la funzione. Quando poi chiamerà Oeq fornendo la preimmagine di y (ovvero x') da lui calcolata, se Oeq appartiene al primo membro dell'equivalenza, allora $\text{Oeq}()$ ritornerà sempre true, mentre se appartiene al secondo ritornerà sempre false. In questo modo A osserva dei comportamenti diversi fra i due game, e quindi può distinguerli. Supponiamo invece che f si effettivamente one-way. Allora non esisterà nessun attaccante efficiente che riesca ad invertire f . L'unico modo che ha quindi un attaccante A per invertire la funzione è chiamare $\text{Ox}()$ e ottenere così una preimmagine valida. Se però l'attaccante chiama $\text{Ox}()$ allora L e R sono indistinguibili (a meno di probabilità trascurabili). Infatti se l' $\text{Ox}()$ chiamato dall'attaccante appartiene ad L allora viene semplicemente ritornata x . Se invece $\text{Ox}()$ appartiene ad R l'oracolo prima di ritornare x assegna a k il valore di una costante, *mark*. Quando poi l'attaccante chiama

Oeq(), nel caso Oeq sia in R allora Oeq effettua il test e se k è stato definito, da una precedente chiamata a Ox(), ritornerà quello che avrebbe ritornato Oeq nel game a sinistra dell'equivalenza; se invece k non è stato definito allora significa che l'attaccante non ha richiamato Oeq e quindi è lecito supporre che non sia riuscito ad invertire f , essendo questa one-way, e quindi Oeq ritorna false. In questo modo i due game sono effettivamente indistinguibili, perchè non presentano differenze di comportamento che A possa notare, e quindi ai suoi occhi sono indistinguibili. Quindi f è indistinguibile *se e solo se* f è one-way; quindi la precedente equivalenza è una definizione ben posta di funzione one-way.

Un'ulteriore definizione viene fornita al CryptoVerif, quella di funzione hash. La funzione hash viene fornita attraverso il seguente codice:

```

equiv
foreach iH  $\leq$  nH do OH(x:hashinput) := return(hash(x));
 $\approx_{pow}$ 
foreach iH  $\leq$  nH do OH(x:hashinput) := find u  $\leq$  nH suchthat (defined(x[u],r[u])
 $\wedge$  x = x[u]) then return(r[u])
else r  $\leftarrow$  R hashoutput; return(r).
  let hashoracle = foreach iH  $\leq$  qH do OH(x:hashinput) := return(hash(x)).

```

La funzione hash è intesa implementata nel modello dell'oracolo random. Ovvero la funzione se non è mai stata richiamata su un particolare valore x_0 allora ritorna un valore casuale, altrimenti ritorna il valore che ha ritornato precedentemente. Questo viene fatto salvando il valore ritornato per un particolare input in un array, e poi al momento della chiamata effettuando un look up nell'array.

Infine abbiamo delle semplici regole di riscrittura che servono a descrivere alcune proprietà delle funzioni in gioco. Per esempio:

```

forall r:seed, x:D, x':D; (x' = invf(skgen(r),x)) = (f(pkgen(r),x') = x).
forall r:seed, x:D; f(pkgen(r), invf(skgen(r), x)) = x.
forall r:seed, x:D; invf(skgen(r), f(pkgen(r), x)) = x.

```

Le precedenti regole servono a definire *invf* come funzione inversa di f e viceversa. Mentre le seguenti:

```

forall k:skey, x:D, x':D; (invf(k,x) = invf(k,x')) = (x = x').
forall k:pkey, x:D, x':D; (f(k,x) = f(k,x')) = (x = x').
forall k:pkey, x:D, x':D; (f'(k,x) = f'(k,x')) = (x = x').

```

modellano l'iniettività delle funzioni $invf$, f' , f'^8 .

Con il comando: `./cryptoverif -in oracles -lib default fdh Si`

⁸Non serve ai fini della dimostrazione modellare l'iniettività della funzione $invf'$.

Capitolo 4

Risultati Raggiunti

Capitolo 5

Conclusioni

Bibliografia

- [AG99] Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. *Inf. Comput.*, 148(1):1–70, 1999.
- [AR07] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *J. Cryptology*, 20(3):395, 2007.
- [BAN90] Michael Burrows, Martín Abadi, and Roger M. Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 8(1):18–36, 1990.
- [BJST08] Bruno Blanchet, Aaron D. Jaggar, Andre Scedrov, and Joe-Kai Tsay. Computationally sound mechanized proofs for basic and public-key Kerberos. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, pages 87–99, Tokyo, Japan, March 2008. ACM.
- [BP06] Bruno Blanchet and David Pointcheval. Automated security proofs with sequences of games. In Cynthia Dwork, editor, *CRYPTO'06*, volume 4117 of *Lecture Notes on Computer Science*, pages 537–554, Santa Barbara, CA, August 2006. Springer Verlag.
- [DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.
- [Dwo06] Cynthia Dwork, editor. *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*. Springer, 2006.
- [Gol00] Oded Goldreich. *Foundations of Cryptography: Basic Tools*. Cambridge University Press, New York, NY, USA, 2000.

- [Kem87] Richard A. Kemmerer. Analyzing encryption protocols using formal verification authentication schemes. In *CRYPTO*, pages 289–305, 1987.
- [KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.
- [Pau98] Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6(1-2):85–128, 1998.
- [Sho] Victor Shoup. Sequences of games: A tool for taming complexity in security proofs. <http://eprint.iacr.org/2004/332.pdf>.