13 Firma Digitale

13.1 Sistemi di Firma

Un sistema di firma è un metodo per firmare i messaggi in formato elettronico in modo da poterli trasmettere attraverso una rete di computer. Le differenze sostanziali con la firma convenzionale sono:

1. La firma convenzionale è allegata fisicamente al documento fisico da firmare, invece quella digitale è collegata in modo opportuno al documento elettronico attraverso un opportuno algoritmo.

2. La verifica della firma convenzionale avviene attraverso la comparazione con quella originale (ciò la rende facilmente falsificabile), invece quella digitale usando un algoritmo pubblico noto (ciò la rende, con le dovute attenzioni, difficile da falsificare).

3. Nel caso della firma convenzionale una copia del un documento firmato è distinguibile dall'originale. Contrariamente alla firma convenzionale, una copia della firma digitale è perfettamente identica all'originale. Quindi, nel caso della firma digitale bisogna prevenire che questa venga riutilizzata maliziosamente.

Forniamo una definizione formale di un sistema di firma

Definizione 13.1. **(Sistema di Firma)**
Un **Sistema di Firma** è un quintupla $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ di insiemi finiti e non vuoti soddisfacenti alle seguenti condizioni:

1. $\mathcal{P}$ è l'insieme dei possibili **messaggi**.
2. $\mathcal{A}$ è l'insieme delle possibili **firme**.
3. $\mathcal{K}$ è l'insieme delle possibili **chiavi**.
4. Per ogni $K \in \mathcal{K}$ ci sono un **algoritmo di firma** $\text{sig}_K \in \mathcal{S}$ ed un corrispondente **algoritmo di verifica** $\text{ver}_K \in \mathcal{V}$, dove

$$\begin{aligned} \text{sig}_K &: \mathcal{P} \longrightarrow \mathcal{A} \\ \text{ver}_K &: \mathcal{P} \times \mathcal{A} \longrightarrow \{vero, falso\} \end{aligned}$$

sono funzioni tali che per $(x, y) \in \mathcal{P} \times \mathcal{A}$ vale che

$$\text{ver}_K(x, y) = vero \iff y = \text{sig}_K(x).$$

La coppia (x, y) è detta **messaggio firmato**.

Fissato $K \in \mathcal{K}$ devono valere le seguenti proprietà:

- sig_K e ver_K devono avere complessità computazionale polinomiale, quindi devono essere efficienti come algoritmi.
- L'algoritmo sig_K è **segreto**, invece ver_K è **pubblico**. Inoltre deve essere computazionalmente difficile per un potenziale avversario di determinare una firma y tale che $\text{ver}_K(x, y) = vero$ (si noti che ci possono essere più di una firma valida y per un fissato messaggio x).
- Se un potenziale avversario è in grado di determinare (x, y) con $\text{ver}_K(x, y) = vero$ e x non precedentemente firmato da una delle parti oneste, allora y è detta **falsificazione**.

Il seguente esempio mostra come il crittosistema RSA possa essere utilizzato per fornire un sistema di firma digitale.

Definizione 13.2. **(Sistema di Firma RSA)**
Siano $n = pq$ con p, q primi distinti. Siano $\mathcal{P} = \mathcal{A} = \mathbb{Z}_n$ e

$$\mathcal{K} = \{(n, p, q, d, e) : n = pq \text{ e } ed \equiv 1 \ mod \ \varphi(n)\}$$

allora (n, e) sono pubblici e (p, q, d) privati.
Fissato $K = (n, p, q, e, d)$, per ogni $x, y \in \mathbb{Z}_n$ definiamo

$$\begin{aligned} \text{sig}_K(x) &= x^d \ mod \ n \\ \text{ver}_K(x, y) &= vero \iff x \equiv y^e \ mod \ n. \end{aligned}$$

1. L'utente A firma un messaggio il messaggio x con la funzione di decifratura d_{K_A}, essendo $\text{sig}_{K_A} = d_{K_A}$. È l'unica persona che può creare la firma essendo $\text{sig}_{K_A} = d_{K_A}$ privata.
2. A trasmette (x, y), dove $y = d_{K_A}(x)$ all'utente B
3. Una volta ricevuto il messaggio firmato (x, y), l'utente B utilizza la chiave pubblica $e_{K_A} = \text{ver}_{K_A}$ per calcolare $x = e_{K_A}(y)$.

La firma dell'utente A può essere 'falsificata' come segue dall'avversario C. Fissa y e calcola $x = e_{K_A}(y)$ essendo e_{K_A} pubblica. Quindi, y è una firma valida per il messaggio x, infatti $x = d_{K_A}(y)$. Tuttavia la probabilità che il messaggio x abbia un significato è molto bassa. Viceversa, per determinare un messaggio firmato (x, y) partendo da x bisogna violare il crittosistema RSA.

13.2 Combinare la firma digitale e la crittografia a chiave pubblica

L'utente A vuole trasmettere un messaggio all'utente B.

- A **firma e poi cifra** il messaggio da trasmettere a B (metodo raccomandato).

  1. L'utente A firma un messaggio x con la funzione di decifratura d_{K_A}, essendo $\text{sig}_{K_A} = d_{K_A}$. Quindi il messaggio firmato è $(x, d_{K_A}(x))$.
  2. A cifra $(x, d_{K_A}(x))$ con la funzione di cifratura pubblica e_{K_B} di B, e trasmette a B la coppia $(e_{K_B}(x), e_{K_B}(d_{K_A}(x)))$.
  3. Una volta ricevuto il messaggio prima firmato e poi criptato firmato $(e_{K_B}(x), e_{K_B}(d_{K_A}(x)))$, l'utente B utilizza la sua firma segreta d_{K_B} per recuperare $(x, d_{K_A}(x))$ e poi la funzione di cifratura pubblica di e_{K_A} per verificare la firma di A, ovvero che $x = e_{K_A}(d_{K_A}(x))$.

- A **cifra e poi firma** il messaggio da trasmettere a B (metodo non raccomandato).

  1. L'utente A cifra un messaggio x con e_{K_B} attraverso la chiave pubblica di B e successivamente lo firma con la sua chiave segreta d_{K_A}. Quindi, trasmette a B il messaggio cifrato e firmato $(e_{K_B}(x), d_{K_A}(e_{K_B}(x)))$.
  2. Una volta ricevuto il messaggio, l'utente B usa prima la propria chiave privata d_{K_B} ottenendo così $(x, d_{K_A}(x))$ $(e_{K_B}(x), d_{K_A}(e_{K_B}(x)))$.
  3. Infine, B usa la funzione di cifratura pubblica di e_{K_A} per verificare $x = e_{K_A}(d_{K_A}(x))$.

Il secondo metodo non è raccomandato perché è suscettibile del seguente attacco:

1. L'utente A cifra un messaggio x con e_{K_B} attraverso la chiave pubblica di B e successivamente lo firma con la sua chiave segreta d_{K_A}. Quindi, trasmette a B il messaggio cifrato e firmato $(e_{K_B}(x), d_{K_A}(e_{K_B}(x)))$.

2. Un utente malizioso C, intercettato $(e_{K_B}(x), d_{K_A}(e_{K_B}(x)))$, trasmette $(e_{K_B}(x), d_{K_C}(e_{K_B}(x)))$ all'utente B.

3. Una volta ricevuto il messaggio, l'utente B usa prima la propria chiave privata d_{K_B} ottenendo così $(x, d_{K_C}(x))$. C intercetta il messaggio $(x, d_{K_C}(x))$ e successivamente calcola $x = e_{K_C}(d_{K_C}(x))$. Quindi, B ne deduce che il testo in chiaro x, che C non conosce, è stato trasmesso da C.

13.3 Requisiti di sicurezza per i sistemi di firma

In questa sezione analizziamo quando un sistema si firma è 'sicuro'. L'analisi vine fatta rispetto ai seguenti modelli di attacco:

- **Attacco basato sulla conoscenza della chiave.**
  L'avversario solo conosce la chiave pubblica ver_K.
- **Attacco basato sulla conoscenza di messaggi.**
  L'avversario conosce una lista di messaggi firmati $(x_1, y_1), ..., (x_q, y_q)$ da un utente, i.e $y_i = \text{sig}_K(x_i)$ con $i = 1, ..., q$.
- **Attacco basato sulla conoscenza di messaggi scelti.**
  L'avversario chiede conosce una lista di messaggi firmati $(x_1, y_1), ..., (x_q, y_q)$ da un utente, i.e $y_i = \text{sig}_K(x_i)$ con $i = 1, ..., q$, in cui $x_1, ..., x_q$ sono messaggi scelti dallo stesso stesso avversario.

I possibili obiettivi dell'avversario sono:

- **Decifratura totale.**
  L'avversario determina la funzione sig_K, quindi crea firme valide su un qualsiasi messaggio.
- **Falsificazione selettiva.**
  La probabilità con cui un avversario è capace di creare una firma valida su un messaggio scelto da un (altro) utente non è trascurabile. Cioè, se x è un messaggio scelto da un utente, allora un avversario produce una firma y per x tale che
  $$P[(x, y) : \text{ver}_K(x, y) = vero] >> 0.$$
- **Falsificazione esistenziale.**
  L'avversario crea una firma valida per almeno un messaggio. Cioè crea un a coppia (x, y) dove x messaggio non precedentemente firmato da un altro utente e $\text{ver}_K(x, y) = vero$.

I sistemi di firma non sono incondizionatamente sicuri poiché per un qualsiasi messaggio x un avversario testa tutti i possibili $y \in \mathcal{A}$ fino a che non trova che $\text{ver}_K(x, y) = vero$, essendo ver_K pubblico. Quindi, avendo un tempo sufficiente a disposizione, un avversario può sempre falsificare una firma. Pertanto, l'obiettivo è costruire sistemi di firma che sono computazionalmente sicuri o dimostrabilmente sicuri.

Vediamo i concetti sopra descritti applicati al Sistema di Firma RSA

- **Falsificazione esistenziale basata sulla sola conoscenza della chiave (pubblica):**
  L'avversario sceglie una firma y e calcola $x = e_K(y)$ essendo e_K pubblica. Quindi, y è una firma valida per il messaggio x, infatti $x = d_K(y)$, i.e. $\text{ver}_K(x, y) = vero$.

- **Falsificazione esistenziale basata sulla conoscenza di messaggi:**
  L'avversario i messaggi firmati $(x_1, y_1), (x_2, y_2)$, quindi $y_i = x_i^d \ mod \ n$, $i = 1, 2$, allora $y_1 y_2 = x_1^d x_2^d \ mod \ n$ è una firma valida per il messaggio $x_1 x_2$.

- **Falsificazione selettiva basata sulla conoscenza di messaggi scelti:**
  L'avversario vuole creare la firma per un messaggio x scelto da un utente. Allora determina $x_1, x_2 \in \mathbb{Z}_n$ tali che $x = x_1 x_2 \ mod \ n$ e chiede all'utente di firmare x_1 e x_2. Quindi, procedendo come nel caso precedente, se $y_i = x_i^d \ mod \ n$, $i = 1, 2$, allora $y_1 y_2 = x^d \ mod \ n$ è una firma valida per il messaggio x.

13.4 Sistemi di firma e funzioni Hash

I sistemi di firma sono quasi sempre usati congiuntamente ad una funzione hash crittografica pubblica molto veloce.

La funzione hash $h : \{0,1\}^* \longrightarrow \mathcal{Z}$ dove $\mathcal{Z}$ è un insieme di stringhe di lunghezza binaria fissata, generalmente di 160 bit e il sistema di firma $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ è tale che $\mathcal{Z} \subseteq \mathcal{P}$. Quindi un utente invece di firmare un messaggio, firma il suo sunto. Gli utenti applicano il seguente protocollo:

1. L'utente A sceglie un messaggio x e ne calcola il sunto $z = h(x)$.
2. A sceglie una chiave segreta K e firma z, cioè calcola $y = \text{sig}_K(z)$, e successivamente trasmette la coppia (x, y).
3. Una volta ricevuto (x, y), il destinatario prestabilito B calcola $z = h(x)$, essendo h pubblica e successivamente verifica la firma di A, cioè calcola $\text{ver}_K(z, y) = vero$.

E' importante prestare attenzione all'utilizzo della funzione hash h al fine di non indebolire la sicurezza del sistema di firma $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$. Generalmente, perchè la sicurezza del sistema di firma sia preservata è sufficiente che h sia resistente rispetto ai problemi dell'immagine inversa, della seconda immagine inversa, o della collisione al fine. Infatti,

- **Le falsificazioni esistenziali usando un attacco basato sulla conoscenza di messaggi sono impedite se h è resistente alla seconda immagine inversa.**
  Se così non fosse e un avversario ha sia un messaggio firmato (x, y), i.e. $y = \text{sig}_K(h(x))$ da un generico utente e sia inoltre capace di terminare $x' \neq x$ tale che $h(x') = h(x)$, allora esso determina la falsificazione (x', y) essendo $y = \text{sig}_K(h(x)) = \text{sig}_K(h(x'))$.

- **Le falsificazioni esistenziali usando un attacco basato sulla conoscenza di messaggi scelti sono impedite se h è resistente alla collisione.**
  In questo caso l'avversario determina x, x' distinti e tali che $h(x) = h(x')$. Quindi, chiede ad un utente di firmare x, ottenendo $y = \text{sig}_K(h(x))$. Allora genera la falsificazione (x', y).

- **Le falsificazioni esistenziali usando un attacco basato sulla conoscenza della chiave (pubblica) sono impedite se h è resistente all'immagine inversa.**
  Se l'avversario è capace di calcolare la firma y ad un elemento di $\mathcal{Z}$ ed è in grado di determinare un messaggio x tale che $z = h(x)$, allora (x, y) è una falsificazione.

13.5 Sistema di Firma di ElGamal

Il seguente sistema di Firma dovuto ad ElGamal non è deterministico. Quindi ci sono più firme valide per un qualsiasi messaggio e l'algoritmo di verifica delle firme le deve accettare tutte.

Definizione 13.3. **(Sistema di Firma di ElGamal (1985))**
Sia p un primo tale che il PLD sia intrattabile in $\mathbb{Z}_p^*$ e sia α un elemento primitivo di $\mathbb{Z}_p^*$. Siano $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{A} = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$ e

$$\mathcal{K} = \left\{(p, \alpha, d, \beta) : \beta \equiv \alpha^d \ mod\ p\right\}$$

Allora, la terna (p, α, β) è pubblica, invece d è segreto.
Per ogni $K = (p, \alpha, d, \beta)$ e per ogni random $k \in \mathcal{U}(\mathbb{Z}_{p-1})$, si definisce

$$\text{sig}_K(x, k) = (\gamma, \delta)$$

dove

$$(\gamma, \delta) = (\alpha^k \ mod\ p, (x - d \times \alpha^k \ mod\ p)k^{-1} \ mod\ (p-1)).$$

Per ogni $x, \gamma \in \mathbb{Z}_p^*$ e $\delta \in \mathbb{Z}_{p-1}$ definiamo

$$\text{ver}_K(x, (\gamma, \delta)) = vero \iff \beta^\gamma \gamma^\delta \equiv \alpha^x \ mod\ p.$$

Proposizione 13.4. Vale che

$$\mathrm{ver}_K(x,(\gamma,\delta)) = vero \iff \beta^\gamma \gamma^\delta \equiv \alpha^x \ mod\ p.$$

Dimostrazione. Supponiamo che $\mathrm{ver}_K(x,(\gamma,\delta)) = vero$, dove

$$(\gamma,\delta) = (\alpha^k \ mod\ p, (x - d \times \alpha^k \ mod\ p)k^{-1} \ mod\ (p-1)).$$

Allora

$$\begin{aligned} \beta^\gamma \gamma^\delta &= \alpha^{d(\alpha^k \ mod\ p)} \alpha^{k[\theta(p-1)+(x-d\times\alpha^k \ mod\ p)k^{-1}]} \\ &= \alpha^{d(\alpha^k \ mod\ p)} \alpha^{k\theta(p-1)} \alpha^x \alpha^{-d(\alpha^k \ mod\ p)} \\ &= \alpha^{k\theta(p-1)} \alpha^x \\ &= \alpha^x. \end{aligned}$$

Se $\beta^\gamma \gamma^\delta \equiv \alpha^x \ mod\ p$ e γ è un generatore della parte moltiplicativa del campo, allora esistono interi d e k tali $\beta \equiv \alpha^d \ mod\ p$ e $\gamma \equiv \alpha^k \ mod\ p$.

$$\alpha^{d(\alpha^k \ mod\ p)} \alpha^{k\delta} \equiv \alpha^x \ mod\ p$$

e quindi

$$\alpha^{d(\alpha^k \ mod\ p)+k\delta} \equiv \alpha^x \ mod\ p$$

che è equivalente a

$$x = (d\,(\alpha^x \ mod\ p) + k\delta) \ mod\ (p-1)$$

ovvero, tenendo presente che $k \in \mathcal{U}(\mathbb{Z}_{p-1})$,

$$\delta \equiv (x - d \times \alpha^k \ mod\ p)k^{-1} \ mod\ (p-1).$$

Quindi, $\mathrm{sig}_K(x) = (\gamma,\delta)$, cioè $\mathrm{ver}_K(x,(\gamma,\delta)) = vero$.

□

Esempio 13.5. Sia $p = 467$, $\alpha = 2$, $d = 127$ e quindi

$$\beta = 2^{127} \ mod\ 467 = 132$$

Supponiamo che un utente A voglia firmare il messaggio $x = 100$. Quindi, sceglie un intero casuale $k = 213$. Siccome $\gcd(213, 466) = 1$, allora $k \in \mathcal{U}(\mathbb{Z}_{466})$ e quindi

$$k^{-1} \ mod\ 466 = 431.$$

Ne segue che

$$\begin{aligned} \gamma &= 2^{431} \ mod\ 467 = 29 \\ \delta &= ((100 - 127 \times 29) \times 431) \ mod\ 466 = 51 \end{aligned}$$

Quindi

$$\mathrm{sig}_{(467,2,127,132)}(100) = (29,51)$$

siccome $132^{29}29^{51} \equiv 2^{100} \ mod\ 467$, allora

$$\mathrm{ver}_{(467,2,127,132)}(100,(29,51)) = vero.$$

□

13.6 Sicurezza del Sistema di Firma di ElGamal

Supponiamo che un avversario voglia falsificare la firma del generico messaggio senza conoscere d.

1. L'avversario sceglie x, γ e vuole determinare $\delta = \log_\gamma \alpha^x \beta^{-\gamma}$ deve risolvere il PLD in $\mathbb{Z}_p^*$.

2. L'avversario sceglie x, δ e vuole determinare γ allora deve risolvere l'equazione $\beta^\gamma \gamma^\delta \equiv \alpha^x \ mod\ p$ che è risulta difficile da trattare pur non essendo stata ampiamente studiata come al PLD.

3. L'avversario sceglie γ, δ e vuole determinare $x = \log_\alpha \beta^\gamma \gamma^\delta$ in $\mathbb{Z}_p^*$.

4. Falsificazione esistenziale basata sulla sola conoscenza della chiave pubblica: l'avversario vuole determinare γ, δ e x. Ciò è possibile, se $\gamma = \alpha^i \beta^j$ in $\mathbb{Z}_p^*$ con $0 \le i, j \le p-2$ con $\gcd(j, p-1) = 1$, allora

$$\begin{cases} \gamma = \alpha^i \beta^j \ mod\ p \\ \delta = -\gamma j^{-1} \ mod\ (p-1) \\ x = -\gamma i j^{-1} \ mod\ (p-1) \end{cases}$$

   implica

$$\begin{cases} x - i\delta \equiv 0 \ mod\ (p-1) \\ \gamma + j\delta \equiv 0 \ mod\ (p-1) \end{cases}$$

   Pertanto

$$\begin{aligned} \alpha^{x-i\delta} \equiv \beta^{\gamma+j\delta} \ mod\ p &\iff \alpha^x \equiv \beta^\gamma (\alpha^i \beta^j)^\delta \ mod\ p \\ &\iff \alpha^x \equiv \beta^\gamma \gamma^\delta \ mod\ p \end{aligned}$$

   e quindi

$$\mathrm{ver}_K(x, (\gamma, \delta)) = vero.$$

   Così, $\mathrm{sig}_K(x) = (\gamma, \delta)$ ovvero (γ, δ) è una firma valida per il messaggio x.

5. Falsificazione esistenziale basata sulla sola conoscenza di un messaggio firmato: l'avversario vuole determinare una firma valida (γ', δ') per un messaggio x' a partire dal messaggio x con firma (γ, δ).

   Siano h, i, j interi tali che $0 \le h, i, j \le p-2$ e $\gcd(h\gamma - j\delta, p-1) = 1$ e siano

$$\begin{cases} \gamma' = \gamma^h \alpha^i \beta^j \ mod\ p \\ \delta' = \delta\lambda(h\gamma - j\delta)^{-1} \ mod\ (p-1) \\ x' = \gamma^h \alpha^i \beta^j (hx + i\delta)(h\gamma - j\delta)^{-1} \ mod\ (p-1) \end{cases}$$

   È facile vedere che e che quindi (γ', δ') è firma valida per un messaggio x'.

6. La conoscenza da parte dell'avversario dell'intero casuale intero casuale k invertibile nelle classi di resto mod $p-1$ e di un messaggio firmato $(x,(\gamma,\delta))$ implica la conoscenza della chiave segreta

$$d = (x - k\delta)\gamma^{-1}$$

a questo punto l'avversario può creare firme valide a volontà.

7. L'utilizzo dello stesso intero casuale k per determinare per firmare due messaggi distinti implica la determinazione di k e quindi della chiave segreta d.

Supponiamo che (γ,δ_i) sia la firma di x_i, $i = 1,2$. Quindi valgono $\beta^\gamma\gamma^{\delta_1} \equiv \alpha^{x_1} \ mod\ p$ e $\beta^\gamma\gamma^{\delta_2} \equiv \alpha^{x_2} \ mod\ p$.

$$\gamma^{\delta_1-\delta_2} \equiv \alpha^{x_1-x_2} \ mod\ p \Longleftrightarrow \alpha^{k(\delta_1-\delta_2)} \equiv \alpha^{x_1-x_2} \ mod\ p$$

che è equivalente a

$$k(\delta_1 - \delta_2) \equiv (x_1 - x_2) \ mod\ (p-1) \tag{13.1}$$

Sia $D = \gcd(\delta_1 - \delta_2, p-1)$.

Siccome $D \mid \delta_1 - \delta_2$ e $D \mid p-1$, allora $D \mid x_1 - x_2$. Siano

$$\begin{cases} x' = \frac{x_1-x_2}{D} \\ \delta' = \frac{\delta_1-\delta_2}{D} \\ p' = \frac{p-1}{D} \end{cases}$$

allora (13.1) diventa

$$x' \equiv k\delta' \ mod\ p'.$$

Siccome $\gcd(\delta', p') = 1$, allora sia $\varepsilon = \delta'^{-1} \ mod\ p'$ e quindi

$$k = x'\varepsilon \ mod\ p'.$$

Pertanto,

$$k = (x'\varepsilon + ip') \ mod\ (p-1)$$

con $0 \le i \le p'-1$ essendo $p' = \frac{p-1}{D}$. Dei p' candidati valori di k solo uno è corretto che realizza $\gamma \equiv \alpha^k \ mod\ p$ e per tali valore come visto sopra $d = (x_1 - k\delta_1)\gamma^{-1}$.

- Gli attacchi **(1)** – **(3)** sono impediti scegliendo un primo p tale che il PLD sia intrattabile in $\mathbb{Z}_p^*$.
- Per quanto visto, gli attacchi **(4)** e **(5)** sono impediti associando al Sistema di Firma di ElGamal un funzione hash che sia resistente all'immagine inversa e alla seconda immagine inversa, rispettivamente.
- Gli attacchi **(6)** e **(7)** sono impediti mantenendo segreto l'intero random k e usandone uno diverso per ogni messaggio da firmare.

13.7 Varianti del Sistema di firma ElGamal

In molte situazioni un messaggio è cifrato e decifrato solo una volta, quindi è importante che il crittosistema sia sicuro solo al momento della cifratura del messaggio. Un messaggio firmato, invece, ha un valore legale come un contratto o un testamento quindi è necessario verificare la firma anche molti anni dopo che il messaggio è stato firmato. Quindi, bisogna avere molte più precauzioni su un sistema di firma piuttosto che ad un crittosistema. Siccome il sistema di firma di ElGamal fonda la sua sicurezza sul PLD, affinchè questa sia duratura nel nel tempo il modulo p deve essere costituito da 1024 bit (in realtà anche più grande) questo significa che la firma nel sistema di ElGamal è di almeno 2048 bit.

A fine di di rendere la firma notevolmente più corta sono state progettati i seguenti sistemi analizzati singolarmente in seguito:

1. Sistema di Firma di Schnorr.
2. L'algoritmo di firma digitale (DSA).
3. L'algoritmo di firma digitale basato sulle curve ellittiche (ECDSA).

13.7.1 Il Sistema di Firma di Schnorr

Figura 13.1: Claus-Peter Schnorr (1943)

Definizione 13.6. **(Sistema di firma di Schnorr (1990))**
Siano p un primo tale che il PLD sia intrattabile in $\mathbb{Z}_p^*$. Sia q un divisore primo di $p-1$ e sia α una radice q-esima dell'unità, (ovvero, $\alpha = \alpha_0^{\frac{p-1}{q}i}$, $0 \leq i \leq q-1$, dove α_0 è un elemento primitivo di $\mathbb{Z}_p^*$). Siano $\mathcal{P} = \{0,1\}^*$, $\mathcal{A} = \mathbb{Z}_q^2$ e sia

$$\mathcal{K} = \left\{(p, q, \alpha, d, \beta) : \beta \equiv \alpha^d \ mod\ p\right\}$$

dove $0 \leq d \leq q-1$. La quadrupla (p, q, α, β) è pubblica, invece d è segreto. Infine, sia $h : \{0,1\}^* \longrightarrow \mathbb{Z}_q$ una funzione hash sicura. Per ogni $K = (p, q, \alpha, d, \beta)$ e un intero segreto k tale che $1 \leq k \leq q-1$ si definisce

$$\text{sig}_K(x, k) = (\gamma, \delta)$$

dove

$$(\gamma, \delta) = (h(x \parallel \alpha^k), (k + d\gamma) \ mod\ q).$$

Per ogni $x \in \{0,1\}^*$ e $\gamma, \delta \in \mathbb{Z}_q$ definiamo

$$\text{ver}_K(x, (\gamma, \delta)) = vero \Longleftrightarrow h(x \parallel \alpha^\delta \beta^{-\gamma}) = \gamma.$$

Proposizione 13.7. Vale che

$$\text{ver}_K(x, (\gamma, \delta)) = vero \Longleftrightarrow h(x \parallel \alpha^\delta \beta^{-\gamma}) = \gamma.$$

Dimostrazione.

($\Rightarrow$) Supponiamo che $\text{ver}_K(x, (\gamma, \delta)) = vero$, dove

$$(\gamma, \delta) = (h(x \parallel \alpha^k), (k + d\gamma) \ mod\ q).$$

Allora $h(x \parallel \alpha^\delta \beta^{-\gamma}) = \gamma$, se e solo se $x \parallel \alpha^\delta \beta^{-\gamma} = x \parallel \alpha^k$ (in binario). Ciò è equivalente a $\alpha^\delta \beta^{-\gamma} = \alpha^k$, ovvero a

$$\begin{aligned} \delta = k + d\gamma &\Longleftrightarrow \alpha^\delta \alpha^{-d\gamma} \equiv \alpha^k \ mod\ q \\ &\Longleftrightarrow \alpha^\delta \beta^{-\gamma} = \alpha^k. \end{aligned} \tag{13.2}$$

Pertanto, $\alpha^\delta \beta^{-\gamma} \equiv \alpha^k \ mod\ p$ essendo $Z_q \leq \mathbb{Z}_p^*$

($\Leftarrow$) Viceversa $h(x \parallel \alpha^\delta \beta^{-\gamma}) = \gamma$. Siccome $\alpha^\delta \beta^{-\gamma} \in Z_q$ allora esiste un intero $1 \leq k \leq q-1$, tale che $\alpha^\delta \beta^{-\gamma} \equiv \alpha^k \ mod\ q$, e quindi $\delta = k + d\gamma$ per (13.2). Pertanto $\text{sig}_K(x, k) = (h(x \parallel \alpha^k), (k + d\gamma) \ mod\ q)$ e quindi

$$\text{ver}_K(x, (h(x \parallel \alpha^k), (k + d\gamma) \ mod\ q)) = vero.$$

□

Caratteristiche del Sistema di Firma di Schnorr

1. Il Sistema di Firma di Schnorr è una modifica del sistema di Firma di ElGamal con il vantaggio che la firma nel primo caso ha lunghezza binaria molto minore che nel secondo. Infatti, allora la firma nel caso di ElGamal è lunga circa $2\log_2 p$ bit, nel caso di Schonorr è $\log_2 q$ bit dove $q \mid p-1$, anche se i calcoli sono fatti in $\mathbb{Z}_p$. In particolare, se $p \simeq 2^{1024}$ e $q \simeq 2^{160}$ allora $2\log_2 p \simeq 2048$ bit, mentre $\log_2 q \simeq 160$.

2. Generalmente nei i sistemi di firma che usano un funzione hash crittografica, la firma è consequenziale all'applicazione della funzione hash. Nel sistema di firma di Schnorr la funzione hash è integrata direttamente nel sistema di firma.

3. La sicurezza del sistema di firma di Schnorr è basata sull'intrattabilità computazionale del PLD in $Z_q \leq \mathbb{Z}_p^*$.

Esempio 13.8. Sia $q = 101$ e $p = 78q+1 = 7879$, allora 3 è un elemento primitivo di $\mathbb{Z}_{7879}^*$. Quindi

$$\alpha = 3^{78} \ mod\ 7879 = 170$$

è una radice 101-esima dell'unità in $\mathbb{Z}_{7879}^*$. Sia $d = 75$, allora

$$\beta = \alpha^d \ mod\ 7879 = 4567.$$

Sia x il messaggio da firmare e sia $k = 50$ l'intero random segreto scelto dall'utente che vuole firmare x. Allora

$$\alpha^k \ mod\ p = 170^{50} \ mod\ 7879 = 2518$$

in binario

$$\alpha^k \ mod\ p = 100111010110.$$

Sia h una qualsiasi funzione hash e supponiamo per semplicità che $h(x \parallel 100111010110) = 96$. Quindi,

$$\delta = (50 + 75 \times 96) \ mod\ 101 = 79$$

allora

$$\mathrm{sig}_{(7879,101,170,75,4567)}(x, 50) = (96, 79).$$

Siccome $170^{79}4567^{-96} \ mod\ 7879 = 2518$, che in binario è 100111010110, e $h(x \parallel 100111010110) = 96$ allora

$$\mathrm{ver}_{(7879,101,170,75,4567)}(x, (96, 79)) = vero.$$

□

13.7.2 L'Algoritmo di Firma Digitale

Definizione 13.9. **(L'algoritmo di Firma Digitale (1994))**
Sia p un primo di L bit dove $L = 64\theta$ dove $8 \leq \theta \leq 16$ tale che il PLD in $\mathbb{Z}_p^*$ sia intrattabile, e siano q un primo di 160 bit che divide $p-1$ e α una radice q-esima dell'unità in $\mathbb{Z}_p^*$. Siano $\mathcal{P} = \{0,1\}^*$, $\mathcal{A} = \left(\mathbb{Z}_q^*\right)^2$ e

$$\mathcal{K} = \left\{(p, q, \alpha, d, \beta) : \beta \equiv \alpha^d \ mod\ p\right\}$$

dove $0 \leq d \leq q-1$. La quadrupla (p, q, α, β) è pubblica, invece d è segreto. Per ogni $K = (p, q, \alpha, d, \beta)$ e un intero segreto k tale che $1 \leq k \leq q-1$ si definisce

$$\text{sig}_K(x, k) = (\gamma, \delta)$$

dove

$$(\gamma, \delta) = (\alpha^k \ mod\ p \ mod\ q, (\text{SHA}-1(x) + d\gamma)k^{-1} \ mod\ q)$$

(se $\gamma = 0$ o $\delta = 0$, allora viene scelto un nuovo valore di k).
Per ogni $x \in \{0,1\}^*$ e $\gamma, \delta \in \mathbb{Z}_q^*$ vale che

$$\text{ver}_K(x, (\gamma, \delta)) = vero \Longleftrightarrow \alpha^{e_1}\beta^{e_2} \ mod\ p \ mod\ q = \gamma,$$

dove

$$(e_1, e_2) = (\text{SHA}-1(x)\delta^{-1} \ mod\ q, \gamma\delta^{-1} \ mod\ q).$$

Caratteristiche del DSA

1. Il DSA, analogamente al Sistema di Firma di Schnorr, opera in un opportuno sottogruppo Z_q di $\mathbb{Z}_p^*$. Inoltre, le forme delle chiavi nei due sistemi sono uguali.
2. La funzione hash utilizzata nel DSA è la SHA $-$ 1 e la firma consiste di circa 320 bit.
3. La sicurezza del sistema di firma del DSA, come quella di Schnorr, è basata sull'intrattabilità computazionale del PLD in $Z_q \leq \mathbb{Z}_p^*$.
4. Si noti che se un utente ottiene $\delta \equiv 0 \ mod\ q$, dovrebbe eliminarlo e scegliere un nuovo intero random. La probabilità che questo accada è $1/q \simeq 2^{-160}$.

Esempio 13.10. Siano $(p, q, \alpha, d, \beta) = (7879, 101, 170, 75, 4567)$ e $k = 50$ come nell'**Esempio 13.8** e supponiamo che l'utente voglia firmare $\text{SHA}-1(x) = 22$. Allora $k^{-1} \ mod\ 101 = 99$ e

$$\begin{aligned} \gamma &= (170^{50} \ mod\ 7879) \ mod\ 101 = 2518 \ mod\ 101 = 94 \\ \delta &= ((22 + 75 \times 94) \times 99) \ mod\ 101 = 97. \end{aligned}$$

Quindi

$$\text{sig}_{(7879,101,170,75,4567)}(x,50) = (94,97).$$

Allora

$$\begin{aligned} \delta^{-1} &= 97^{-1} \ mod\ 101 = 25 \\ e_1 &= (22 \times 25) \ mod\ 101 = 45 \\ e_2 &= (94 \times 25) \ mod\ 101 = 27 \end{aligned}$$

Siccome

$$\left(170^{45}4567^{27} \ mod\ 7879\right) \ mod\ 101 = 2528 \ mod\ 101 = 94,$$

allora

$$\text{ver}_{(7879,101,170,75,4567)}(x,(94,97)) = vero.$$

□

13.7.3 L'Algoritmo di Firma Digitale basato sulle curve ellittiche (ECDSA)

Definizione 13.11. **(Algoritmo di Firma Digitale basato sulle curve ellittiche (2000))**
Sia $\mathcal{E}$ una curve ellittica su $GF(p)$ dove p è un primo oppure una potenza di 2. Sia Q un punto di $\mathcal{E}$ di ordine un primo q tale che IL PLD sia intrattabile in $\langle Q \rangle$. Siano $\mathcal{P} = \{0,1\}^*$, $\mathcal{A} = \left(\mathbb{Z}_q^*\right)^2$ e

$$\mathcal{K} = \{(p,q,\mathcal{E},Q,m,B) : B = mQ\}$$

dove $0 \leq m \leq q-1$. La quintupla $(p,q,\mathcal{E},Q,B)$ è pubblica, invece m è segreto. Per ogni $K = (p,q,\mathcal{E},Q,m,B)$ e un intero segreto random k tale che $1 \leq k \leq q-1$ si definisce

$$\text{sig}_K(x,k) = (r,s)$$

dove

$$\begin{cases} kQ = (u,v) \\ r = u \ mod\ q \\ s = k^{-1}(\text{SHA}-1(x) + mr) \ mod\ q \end{cases}$$

(se $r = 0$ o $s = 0$, allora viene scelto un nuovo valore di k).
Per ogni $x \in \{0,1\}^*$ e $r,s \in \mathbb{Z}_q^*$ vale che

$$\begin{cases} w = s^{-1} \ mod\ q \\ i = w\,(\text{SHA}-1(x)) \ mod\ q \\ j = wr \ mod\ q \\ (u,v) = iQ + jB \end{cases}$$

allora

$$\text{ver}_K(x,(r,s)) = vero \iff u \ mod\ q = r.$$

Esempio 13.12. Si consideri la curva ellittica $\mathcal{E} : y^2 = x^3 + x + 6$ a coefficienti in $GF(11)$. Sia

$$K = (11, 13, (2, 7), 7, (7, 2))$$

e supponiamo che $\text{SHA} - 1(x) = 4$ e che il generico utente voglia firmare x usando l'intero casuale $k = 3$. Allora

$$\begin{aligned} (u, v) &= 3(2, 7) = (8, 3) \\ r &= 8 \ mod \ 13 = 8 \\ s &= 3^{-1}(4 + 7 \times 8) \ mod \ 13 = 7. \end{aligned}$$

Quindi,

$$\text{sig}_{(11,13,(2,7),7,(7,2))}(x, 3) = (8, 7).$$

Il destinatario del messaggio firmato calcola

$$\begin{cases} w = 7^{-1} \ mod \ 13 = 2 \\ i = (2 \times 4) \ mod \ 13 = 8 \\ j = (2 \times 8) \ mod \ 13 = 3 \\ (u, v) = 8(2, 7) + 3(7, 2) = (8, 3) \end{cases}$$

Siccome $u \ mod \ 13 = 8 = r$, allora

$$\text{ver}_{(11,13,(2,7),7,(7,2))}(x, (8, 7)) = vero$$

dimostra la certezza del mittente.

□

13.8 Il Sistema di Firma di Lamport

Il seguente sistema di firma, dovuto a Lamport, fonda la sua sicurezza su una funzione one-way (cioè è dimostrabilmente sicuro) ed ogni chiave è utilizzata per firmare un unico documento.

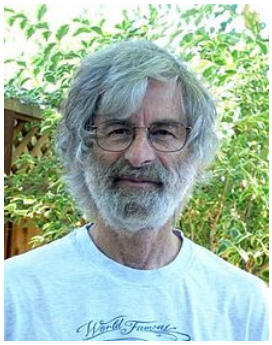

Figura 13.2: Leslie Lamport (1941)

Definizione 13.13. **(Sistema di Firma di Lamport (1976))**
Sia $k \in \mathbb{N}$ e siano $\mathcal{P} = \{0,1\}^k$, $f : Y \longrightarrow Z$ una funzione (pubblica) one-way, $\mathcal{A} = Y^k$ e $\mathcal{K} \subseteq Y^{2k} \times Z^{2k}$. Sia $y_{ij} \in Y$ scelto in modo random, dove $1 \leq i \leq k$ e $j = 0, 1$, e sia $z_{ij} = f(y_{ij})$. Sia

$$K = (y_{10}, ..., y_{k0}, y_{11}, ..., y_{k1}, z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1}),$$

dove

$$(y_{10}, ..., y_{k0}, y_{11}, ..., y_{k1})$$

è privata, invece

$$(z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1})$$

è pubblica. Allora definiamo

$$\text{sig}_K(x_1, ..., x_k) = (y_{1,x_1}, ..., y_{k,x_k}).$$

Una firma $(a_1, ..., a_k)$ su un messaggio $(x_1, ..., x_k)$ è verificata come segue

$$\text{ver}_K((x_1, ..., x_k), (a_1, ..., a_k)) = vero \Longleftrightarrow f(a_i) = z_{i,x_i},\ 1 \leq i \leq k.$$

Remark 13.14. Il sistema di Firma di Lamport può essere costruito a partire da dalla funzione di esponenziazione modulare, che si crede essere one-way: Se p è un primo e α è un elemento primitivo di $\mathbb{Z}_p^*$, allora

$$f : \{0, ..., p-2\} \longrightarrow \mathbb{Z}_p^*, x \longmapsto \alpha^x \ \ mod\ p.$$

Esempio 13.15. Sia $p = 7879$ e $\alpha = 3$ un elemento primitivo di $\mathbb{Z}^*_{7879}$ e sia $k = 3$.

$$f : \{0, ..., 7877\} \longrightarrow \mathbb{Z}^*_{7879}, x \longmapsto 3^x \ \ mod\ 7879.$$

Sia

$$(y_{10}, y_{20}, y_{30}, y_{11}, y_{21}, y_{31}) = (5831, 803, 4285, 735, 2467, 6449)$$

e le rispettive immagini mediante f

$$(z_{10}, z_{20}, z_{30}, z_{11}, z_{21}, z_{31}) = (2009, 4672, 268, 3810, 4721, 5731).$$

Quindi la chiave è

$$\begin{aligned} K = (&5831, 803, 4285, 735, 2467, 6449, \\ &2009, 4672, 268, 3810, 4721, 5731). \end{aligned} \tag{13.3}$$

Supponiamo che l'utente voglia firmare il messaggio $x = (1, 1, 0)$, allora

$$\text{sig}_K(1, 1, 0) = (y_{11}, y_{21}, y_{30}) = (735, 2467, 4285).$$

Il destinatario prestabilito una volta ricevuto il messaggio firmato $((1, 1, 0), (735, 2467, 4285))$ calcola

$$\begin{cases} f(375) = 3^{375} \ \ mod\ 7879 = 3810 \\ f(2467) = 3^{2467} \ \ mod\ 7879 = 4721 \\ f(4285) = 3^{4285} \ \ mod\ 7879 = 268 \end{cases}$$

e verifica in (13.3) che $(3810, 4721, 268) = (z_{11}, z_{21}, z_{30})$. In tal caso,

$$\text{ver}_K((1, 0, 0), (735, 2467, 4285)) = vero.$$

□

1. Se la chiave è utilizzata per firmare più di un messaggio, il sistema di firma di Lamport non è sicuro.

   Infatti, se per esempio $k = 3$ e quindi i seguenti messaggi $x = (0, 1, 1)$ e $x' = (1, 0, 1)$ sono firmati con la stessa chiave

   $$K = (y_{10}, y_{20}, y_{30}, y_{11}, y_{21}, y_{31}, z_{10}, z_{20}, z_{30}, z_{11}, z_{21}, z_{31})$$

   segreta, allora un avversario produce una $(2, 1)$-falsificazione esistenziale. Infatti, se le firma di x è (y_{10}, y_{21}, y_{31}) e quella di x' è (y_{11}, y_{20}, y_{31}), allora l'avversario firma $x'' = (1, 1, 1)$ con (y_{11}, y_{21}, y_{31}) e $x''' = (0, 0, 1)$ con (y_{10}, y_{20}, y_{31}). Entrambe le firme sono valide!

2. Proviamo che il sistema di firma di Lamport è dimostrabilemente sicuro nella modalità **one-time**, cioè la chiave è utilizzata per firmare un solo documento. In particolare, proviamo che sistema è sicuro rispetto all'attacco basato sulla conoscenza della chiave pubblica, se f è biettiva e la chiave pubblica $(z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1})$ è costituita da $2k$ elementi distinti.

   Sia Lamport-Falsificazione un algoritmo deterministico che fornita una chiave pubblica $(z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1})$ restituisce in output la coppie di k-ple $((x_1, ..., x_k), (a_1, ..., a_k))$ dove $f(a_i) = z_{i,x_i}$, $1 \leq i \leq k$. e consideriamo il seguente algoritmo

Algoritmo 13.16. **(Lamport-immagine inversa(z))**

esterni: f, Lamport-Falsificazione

comment: supponiamo che $f : Y \longrightarrow Z$ sia una biiezione

fissati $i_0 \in \{1, ...k\}$ e $j_0 \in \{0, 1\}$ costruiamo una chiave pubblica

$(z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1})$ tale che $z_{i_0 j_0} = z$.

$((x_1, ..., x_k), (a_1, ..., a_k)) \leftarrow$ Lamport-Falsificazione$((z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1}))$

if $x_{i_0} = j_0$

then return (a_{i_0})

else return (insuccesso)

Noi stiamo assumendo che l'algoritmo Lamport-Falsificazione trovi sempre una falsificazione $((x_1, ..., x_k), (a_1, ..., a_k))$ relativa alla chiave pubblica $(z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1})$. Se vale $x_{i_0} = j_0$, allora $f(a_{i_0}) = z_{i_0, x_{i_0}} = z_{i_0, j_0} = z$ e quindi $a_{i_0} \in f^{-1}(z)$, cioè abbiamo trovato un elemento dell'immagine inversa di z. Vogliamo provare nel seguente teorema che la probabilità media di successo nel determinare un elemento dell'immagine inversa di $f^{-1}(z)$, al variare di z in Z è almeno $1/2$.

Teorema 13.17. *Sia $f : Y \longrightarrow Z$ una funzione one-way biiettiva, e supponiamo che esista un algoritmo deterministico Lamport-Falsificazione* (LF) *che produce una falsificazione esistenziale basata sulla sola conoscenza della chiave pubblica nel Sistema di Firma di Lamport per ogni chiave $(z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1}) \in Z^{2k}$ costituita da $2k$ termini distinti. Allora esiste un algoritmo Lamport-immagine inversa* (LII) *che determina immagini inverse di elementi random in Z con probabilità maggiore o uguale a $1/2$.*

Dimostrazione. Sia $\mathcal{S} \subseteq Z^{2k}$ l'insieme di tutte le possibili chiavi pubbliche, e per ogni $z \in Z$ sia S_z l'insieme

$$\{(z_{10}, ..., z_{k0}, z_{11}, ..., z_{k1}) \in \mathcal{S} : \exists i \in \{1, ...k\}, j \in \{1, 2\} \text{ t.c. } z_{ij} = z\}.$$

Denotata con $\mathcal{Z}$ la generica chiave pubblica, allora $\mathcal{T}_z$ è l'insieme degli $\mathcal{Z} \in \mathcal{S}_z$ tale che Lamport-immagine inversa(z) successo, se $\mathcal{Z}$ è scelta come chiave pubblica nell'algoritmo Lamport-immagine inversa, essendo questo randomizzato. Posto $s = |\mathcal{S}|$, $s_z = |\mathcal{S}_z|$ e $t_z = |\mathcal{T}_z|$, contiamo in due modi diversi

$$\sum_{\substack{z \in Z, \mathcal{Z} \in \mathcal{S} \\ \mathcal{Z} \in \mathcal{T}_z}} (\mathcal{Z}, z). \tag{13.4}$$

Fissato $z \in Z$ il numero degli $\mathcal{Z} \in \mathcal{T}_z$ è t_z quindi (13.4) vale $\sum_{z \in Z} t_z$. D'altra parte, fissato $\mathcal{Z} \in \mathcal{S}$ l'algoritmo deterministico Lamport-Falsificazione individua esattamente gli inversi tramite f di k elementi di Z. Quindi esistono esattamente k elementi $z_1, ..., z_k$ di Z tali che $\mathcal{Z} \in \mathcal{T}_{z_j}$, $j = 1, ..., k$. Pertanto, (13.4) vale $\sum_{\mathcal{Z} \in \mathcal{S}} k = ks$. Quindi, vale che

$$\sum_{z \in Z} t_z = ks \tag{13.5}$$

Ora contiamo in due modi diversi

$$\sum_{\substack{z \in Z, \mathcal{Z} \in \mathcal{S} \\ \mathcal{Z} \in \mathcal{S}_z}} (\mathcal{Z}, z). \tag{13.6}$$

Fissato $z \in Z$ il numero degli $\mathcal{Z} \in \mathcal{S}_z$ è s_z quindi (13.4) vale $\sum_{z \in Z} s_z$. D'altra parte, per ipotesi, fissato $\mathcal{Z} \in \mathcal{S}$ il numero degli z che $\mathcal{Z}$ contiene è $2k$ elementi di Z. Quindi, $\sum_{\mathcal{Z} \in \mathcal{S}} 2k = 2ks$. Pertanto si ha

$$\sum_{z \in Z} s_z = 2ks$$

Sia z_0 tale che $s_{z_0} = \max\{s_z : z \in Z\}$. Allora

$$2ks \leq s_{z_0} |Z|$$

Sia p_z la probabilità che l'algoritmo Lamport-immagine inversa(z) abbia successo. Chiaramente, $p_z = t_z / s_z$. Allora,

$$\bar{p} = \frac{1}{|Z|} \sum_{z \in Z} p_z = \frac{1}{|Z|} \sum_{z \in Z} \frac{t_z}{s_z} \geq \frac{1}{|Z| \, s_{z_0}} \sum_{z \in Z} t_z = \frac{ks}{2ks} = \frac{1}{2}.$$

Pertanto, $\bar{p} \geq 1/2$ che è l'asserto.

□

Remark 13.18. Il sistema di Firma di Lamport, sebbene elegante, risulta poco pratico per via della grandezza delle firme che esso produce. Supponiamo per esempio di prendere come f l'esponenziazione modulare (quella utilizzata per il crittosistema RSA). Cioè se Se p è un primo e α è un elemento primitivo di $\mathbb{Z}_p^*$, allora

$$f : \{0, ..., p-2\} \longrightarrow \mathbb{Z}_p^*, x \longmapsto \alpha^x \ \ mod\ p.$$

Per essere sicura $p \simeq 1024$ bit e quindi la firma nel sistema di Lamport deve essere lungo $1024 \times k$ bit.

13.9 Firme non ripudiabili

Le firme non ripudiabili sono state introdotte da **Chaum** e **Van Anterwerpen** nel 1989 e presentano diverse novità:

1. La firma non può essere verificata senza la cooperazione del firmatario: questo protegge il firmatario contro la possibilità che i documenti firmati siano duplicati e distribuiti elettronicamente. La verifica è compiuta attraverso il **protocollo challenge and repsonse**.

2. La firma non può essere ripudiata: il firmatario non può asserire che una firma valida sia stata falsificata o possa fare in modo che la firma non sia verificata. Per prevenire questo tipo avvenimenti, le firme non ripudiabili contengono un **protocollo di disconoscimento** attraverso il quale il firmatario può provare che una firma falsificata è di fatto una falsificazione. (Se il firmatario si rifiuta di prendere parte nel protocollo di disconoscimento ciò viene visto come una prova della validità di una firma).

Figura 13.3: David Lee Chaum (1955)

Come vedremo, i sistemi di firma non ripudiabili consistono di tre componenti:

- Algoritmo di firma.
- Algoritmo di verifica.
- Algoritmo di disconoscimento.

Definizione 13.19. **(Sistema di Firma di Chaum - Van Anterwerpen (1989))**
Sia $p = 2q + 1$ un primo tale che q sia un primo e che il PLD sia intrattabile in $\mathbb{Z}_p^*$. Siano $\alpha \in \mathbb{Z}_p^*$ un elemento di ordine q, $1 \leq m \leq q-1$ e $\beta \equiv \alpha^m \ mod\ p$ e sia $G \cong Z_q \leq \mathbb{Z}_p^*$ (G è il sottogruppo dei quadrati di $\mathbb{Z}_p^*$). Siano $\mathcal{P} = \mathcal{A} = G$ e sia

$$\mathcal{K} = \{(p, \alpha, m, \beta) : \beta \equiv \alpha^m \ mod\ p\}$$

La terna (p, α, β) è la chiave pubblica, m è la chiave privata.
Se $K = (p, \alpha, m, \beta)$ e $x \in G$ si definisca

$$y = \text{sig}_K(x) = x^m \ mod\ p.$$

Per $x, y \in G$ la verifica della firma avviene secondo il seguente protocollo:

1. L'utente B destinatario del documento firmato sceglie in modo random $e_1, e_2 \in \mathbb{Z}_q^*$.
2. L'utente B calcola $c \equiv y^{e_1}\beta^{e_2} \ mod\ p$ e lo trasmette al firmatario A (**challenge**).
3. L'utente A calcola $d \equiv c^{m^{-1} \ mod\ q} \ modp$ e lo trasmette a B (**response**).
4. L'utente B accetta y come firma valida se, e solo se,
$$d \equiv x^{e_1}\alpha^{e_2} \ mod\ p.$$

Proposizione 13.20. Siano $x, y \in G$, $\beta \equiv \alpha^m \ mod\ p$, $c \equiv y^{e_1}\beta^{e_2} \ mod\ p$, $d \equiv c^{m^{-1}} \ mod\ p$, allora

$$y \equiv x^m \ mod\ p \iff d \equiv x^{e_1}\alpha^{e_2} \ mod\ p.$$

Dimostrazione. Da $d \equiv c^{m^{-1} \ mod\ q} \ mod\ p$ e $c \equiv y^{e_1}\beta^{e_2} \ mod\ p$ segue che $d \equiv y^{e_1 m^{-1} \ mod\ q}\beta^{e_2 m^{-1} \ mod\ q} \ mod\ p$ e quindi $d \equiv y^{e_1 m^{-1} \ mod\ q}\alpha^{e_2} \ mod\ p$ essendo $\beta \equiv \alpha^m \ mod\ p$.
Pertanto,

$$\begin{aligned} d \equiv x^{e_1}\alpha^{e_2} \ mod\ p &\iff x^{e_1}\alpha^{e_2} \equiv y^{e_1 m^{-1} \ mod\ q}\alpha^{e_2} \ mod\ p \\ &\iff x^{e_1} \equiv y^{e_1 m^{-1} \ mod\ q} \ mod\ p \end{aligned} \tag{13.7}$$

Siccome $e_1 \in \mathbb{Z}_q$, allora esiste v_1 inverso di e_1 in G. Allora $e_1 v_1 = \theta q + 1$. Pertanto

$$\begin{aligned} x^{e_1} \equiv y^{e_1 m^{-1} \ mod\ q} \ mod\ p &\iff x^{e_1 v_1} \equiv y^{e_1 v_1 m^{-1} \ mod\ q} \ mod\ p \\ &\iff x^{\theta q+1} \equiv y^{(\theta q+1)m^{-1} \ mod\ q} \ mod\ p \\ &\iff x \equiv y^{m^{-1} \ mod\ q} \ mod\ p \\ &\iff y \equiv x^m \ mod\ p. \end{aligned} \tag{13.8}$$

Pertanto, da (13.7) e (13.8) segue l'asserto.

□

Esempio 13.21. Sia $p = 467 = 2 \times 233 + 1$ un primo e sia $\alpha_0 = 2$ un elemento primitivo di $\mathbb{Z}^*_{467}$. Allora $\alpha = \alpha_0^2 = 4$ è un elemento primitivo del sottogruppo $G \cong Z_{233}$ dei quadrati di $\mathbb{Z}^*_{467}$. Sia $m = 101$, allora $\beta \equiv 4^{101} \ mod\ 467 = 449$.

Un utente A vuole firmare un messaggio $x = 119$, allora

$$y = \text{sig}_{(467,4,101,449)}119 = 119^{101} \ mod\ 467 = 129$$

e trasmette il messaggio firmato $(x, y) = (119, 129)$ all'utente B. Una volta ricevuto $(119, 129)$ l'utente B, vuole verificare la firma. Allora B opera come segue

1. sceglie due elementi $e_1 = 38$ e $e_2 = 397$ in $\mathbb{Z}_q$
2. calcola $c = 129^{38}449^{397} \ mod\ 467 = 13$ e lo trasmette ad A
3. A calcola $d = 13^{101^{-1} \ mod\ 233} \ mod\ 467 = 13^{30} \ mod\ 467 = 9$ e lo ritrasmette a B.
4. B calcola $109^{38}4^{397} \ mod\ 467 = 9$ che è uguale a $d = 9$ trasmesso da A e quindi è sicuro che la firma è valida, cioè

$$\text{ver}_{(467,4,101,449)}(119, 129) = vero.$$

□

Adesso proviamo che è molto bassa la probailità che un utente A inganni un utente B facendo accettare come valida una firma falsa. Il seguente risultato è indipendente dalle risorse computazionali dell'avversario (l'utente A), cioè la sicurezza è incondizionata.

Proposizione 13.22. Valgono i seguenti fatti:

1. Se vale $c \equiv y^{\bar{e}_1}\beta^{\bar{e}_2} \ mod\ p$, allora q è il numero delle coppie $(e_1, e_2) \in \mathbb{Z}_q^2$ tale che $c \equiv y^{e_1}\beta^{e_2} \ mod\ p$.
2. Se vale **(1)** e $y \not\equiv x^m \ mod\ p$, allora esiste un'unica coppia (e_1, e_2) (tra le q coppie) tale che

$$\begin{cases} c \equiv y^{e_1}\beta^{e_2} \ mod\ p \\ d \equiv x^{e_1}\alpha^{e_2} \ mod\ p \end{cases} \tag{13.9}$$

Dimostrazione. Sia $(\bar{e}_1, \bar{e}_2)$ una coppia tale $c \equiv y^{\bar{e}_1}\beta^{\bar{e}_2} \ mod\ p$. Siccome G è ciclico di ordine primo q esiste un intero k tale che $y \equiv \beta^k \ mod\ q$. Quindi, $y \equiv \beta^k \ mod\ p$, essendo $G \leq \mathbb{Z}^*_p$. Pertanto, $c \equiv \beta^{k\bar{e}_1+\bar{e}_2} \ mod\ p$, allora $(e_1, k\bar{e}_1 + \bar{e}_2 - ke_1)$ è tale che $c \equiv y^{e_1}\beta^{k\bar{e}_1+\bar{e}_2-ke_1} \ mod\ p$. Pertanto, fissata una coppia esistono esattamente q coppie (e_1, e_2) tali che $y^{e_1}\beta^{e_2} \ mod\ p \equiv y^{\bar{e}_1}\beta^{\bar{e}_2} \ mod\ p \equiv c$, che è l'asserto **(1)**.

Supponiamo che valga **(1)** e $y \notin x^m \mod p$, poiché α è un generatore di G, allora esistono $0 \leq i, j, k, \ell \leq q-1$ tale che $c = \alpha^i$, $d = \alpha^j$, $x = \alpha^k$ e $y = \alpha^\ell$. Siccome $G \leq \mathbb{Z}_p^*$, le precedenti uguaglianze sono da intendersi modulo p. Quindi

$$\begin{cases} c \equiv y^{e_1}\beta^{e_2} \mod p \\ d \equiv x^{e_1}\alpha^{e_2} \mod p \end{cases} \iff \begin{cases} \alpha^i \equiv \alpha^{\ell e_1 + m e_2} \mod p \\ \alpha^j \equiv \alpha^{k e_1 + e_2} \mod p \end{cases}$$

che è equivalente a

$$\begin{cases} i \equiv \ell e_1 + m e_2 \mod q \\ j \equiv k e_1 + e_2 \mod q \end{cases} \tag{13.10}$$

siccome $o(\alpha) = q$. Il sistema è lineare nelle indeterminate e_1, e_2 e a coefficienti nel campo $\mathbb{Z}_q$, essendo q primo. Siccome $y \notin x^m \mod p$ e poichè $G \leq \mathbb{Z}_p^*$, allora $\alpha^\ell \notin \alpha^{km} \mod p$ e quindi $\ell - km \not\equiv 0 \mod q$, ovvero

$$\det \begin{pmatrix} \ell & m \\ k & 1 \end{pmatrix} = \ell - km \not\equiv 0 \mod q,$$

allora il sistema (13.10) ammette un'unica soluzione. Pertanto, fissato d esiste un unica coppia (e_1, e_2) tale che valga

$$\begin{cases} c \equiv y^{e_1}\beta^{e_2} \mod p \\ d \equiv x^{e_1}\alpha^{e_2} \mod p. \end{cases}$$

□

Teorema 13.23. *Se $y \notin x^m \mod p$, allora la probabilità che l'utente B accetti y come firma valida per il messaggio x è $1/q$.*

Dimostrazione. Supponiamo che A inganni B trasmettendo la coppia (x, y) con $y \notin x^m \mod p$ firma non valida. Allora, nel protocollo challenge and response vale che:

1. L'utente B sceglie in modo random $\bar{e}_1, \bar{e}_2 \in \mathbb{Z}_q$.
2. L'utente B calcola $c \equiv y^{\bar{e}_1}\beta^{\bar{e}_2} \mod p$ e lo trasmette ad A.
3. L'utente A **sceglie** $\bar{d}$ e lo trasmette a B.
4. L'utente B accetta y come firma valida se, e solo se,
$$\bar{d} \equiv x^{e_1}\alpha^{e_2} \mod p.$$

Quindi la probabilità che B accetti y come firma valida è uguale alla probabilità che $(\bar{e}_1, \bar{e}_2)$ scelti da B coincidano con la soluzione del sistema (13.9)

$$\begin{cases} c \equiv y^{e_1}\beta^{e_2} \mod p \\ \bar{d} \equiv x^{e_1}\alpha^{e_2} \mod p. \end{cases}$$

che per la **Proposizione 13.22** è $1/q$.

□

Analizziamo ora il Protocollo di disconoscimento che consiste nell'applicare il protocollo di verifica due volte.

Algoritmo 13.24. **(Disconoscimento)**

1. L'utente B sceglie in modo random $e_1, e_2 \in \mathbb{Z}_q^*$.
2. L'utente B calcola $c = y^{e_1}\beta^{e_2} \mod p$ e lo trasmette al firmatario A.
3. L'utente A calcola $d = c^{m^{-1} \mod q} \mod p$ e lo trasmette a B.
4. L'utente B verifica $d \not\equiv x^{e_1}\alpha^{e_2} \mod p$.
5. L'utente B sceglie in modo random $f_1, f_2 \in \mathbb{Z}_q^*$.
6. L'utente B calcola $C = y^{f_1}\beta^{f_2} \mod p$ e lo trasmette al firmatario A.
7. L'utente A calcola $D = C^{m^{-1} \mod q} \mod p$ e lo trasmette a B.
8. L'utente B verifica $D \not\equiv x^{f_1}\alpha^{f_2} \mod p$.
9. L'utente B conclude che y è una falsificazione se, e solo se, $(d\alpha^{-e_2})^{f_1} \equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p$.

Sia negli step **1**–**4** e che in quelli **5**–**8** si applica l'algoritmo di verifica, lo step **9** rappresenta una verifica di omogeneità e premette all'utente B di capire se l'utente A produce le risposte nella maniera specificata dal protocollo.

Proviamo i seguenti fatti:

1. L'utente A è in grado di convincere l'utente B che una firma non valida è una falsificazione.
2. La probabilità che l'utente A sia in grado di convincere l'utente B che una firma valida è una falsificazione è molto bassa.

Teorema 13.25. *Se $y \not\equiv x^m \mod p$ e gli utenti A e B seguono il protocollo di disconoscimento, allora*

$$(d\alpha^{-e_2})^{f_1} \equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p.$$

Dimostrazione. Siccome vale che

$$\begin{cases} d \equiv c^{m^{-1} \mod q} \mod p \\ c \equiv y^{e_1}\beta^{e_2} \mod p \\ \beta \equiv \alpha^m \mod p \end{cases}$$

allora

$$\begin{aligned}(d\alpha^{-e_2})^{f_1} &\equiv \left((y^{e_1}\beta^{e_2})^{m^{-1} \bmod q}\alpha^{-e_2}\right)^{f_1} \bmod p \\ &\equiv y^{e_1 f_1 (m^{-1} \bmod q)}\beta^{e_2 f_1 (m^{-1} \bmod q)}\alpha^{-e_2 f_1} \bmod p \\ &\equiv y^{e_1 f_1 (m^{-1} \bmod q)}\alpha^{e_2 f_1}\alpha^{-e_2 f_1} \bmod p \\ &\equiv y^{e_1 f_1 (m^{-1} \bmod q)} \bmod p.\end{aligned}$$

quindi,

$$(d\alpha^{-e_2})^{f_1} \equiv y^{e_1 f_1 (m^{-1} \bmod q)} \bmod p. \tag{13.11}$$

Analogamente,

$$\begin{cases} D \equiv C^{m^{-1} \bmod q} \bmod p \\ C \equiv y^{f_1}\beta^{f_2} \bmod p \\ \beta \equiv \alpha^m \bmod p \end{cases}$$

implica

$$\left(D\alpha^{-f_2}\right)^{e_1} \equiv y^{e_1 f_1 (m^{-1} \bmod q)} \bmod p. \tag{13.12}$$

Da (13.11) e (13.12), segue la tesi.

□

Esempio 13.26. Sia $p = 467$, $\alpha = 4$ un generatore di G il sottogruppo dei quadrati di $\mathbb{Z}^*_{467}$, $m = 101$ e $\beta = 449$. Supponiamo che l'utente A voglia ingannare l'utente B. Sia $y = 83$ la firma **fasulla** dell'utente A al messaggio $x = 286$.

1. L'utente B sceglie $e_1 = 45$ e $e_2 = 237$ in $\mathbb{Z}^*_{233}$.
2. L'utente B calcola $c = 83^{45}449^{237} \bmod 467 = 305$ e lo trasmette ad A.
3. L'utente A calcola $d = 305^{101^{-1} \bmod 233} \bmod 467 = 109$ e lo trasmette a B.
4. L'utente B calcola $286^{45}4^{237} \bmod 467 = 149 \neq 109$.
5. L'utente B sceglie $f_1 = 125$ e $f_2 = 9$ in $\mathbb{Z}^*_{233}$.
6. L'utente B calcola $C = 83^{125}449^{9} \bmod 467 = 270$ e lo trasmette ad A.
7. L'utente A calcola $D = 270^{101^{-1} \bmod 233} \bmod 467 = 68$ e lo trasmette a B.
8. L'utente B calcola $286^{125}4^{9} \bmod 467 = 25 \neq 68$.
9. L'utente B calcola $\left(109 \times 4^{-237}\right)^{125} \bmod 467 = 188$ e $\left(68 \times 4^{-9}\right)^{45} \bmod 467 = 188$ e si convince che la firma dell'utente A è falsa.

□

Analizziamo il caso in cui l'utente A ripudi una firma valida, ovvero $y \equiv x^m \bmod p$, e quindi produca d e D **non** seguendo il protocollo, cioè tali che

$$\begin{cases} d \not\equiv x^{e_1}\alpha^{e_2} \bmod p \\ D \not\equiv x^{f_1}\alpha^{f_2} \bmod p \\ (d\alpha^{-e_2})^{f_1} \not\equiv \left(D\alpha^{-f_2}\right)^{e_1} \bmod p. \end{cases} \tag{13.13}$$

Teorema 13.27. *Supponiamo che $y \equiv x^m \ mod\ p$ e che l'utente B segua il protocollo di disconoscimento. Se $d \not\equiv x^{e_1}\alpha^{e_2} \ mod\ p$ e $D \not\equiv x^{f_1}\alpha^{f_2} \ mod\ p$, allora*

$$\mathbf{P}\left[D\alpha^{-f_2} \equiv (d\alpha^{-e_2})^{f_1/e_1} \ mod\ p\right] = 1/q.$$

Dimostrazione. Sia E_1 l'evento $(d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1} \ mod\ p$. Allora $D\alpha^{-f_2} \equiv (d\alpha^{-e_2})^{f_1/e_1} \ mod\ p$ e quindi

$$D \equiv {d_0}^{f_1}\alpha^{f_2} \ mod\ p \text{ e } d_0 = d^{1/e_1}\alpha^{-e_2/e_1}.$$

Se E_2 denota l'evento $y \equiv d_0^m \ mod\ p$, proviamo che $\mathbf{P}[E_1 \cap E_2] = 0$. Infatti, se $\mathbf{P}[E_1 \cap E_2] > 0$ allora vale che

$$\begin{cases} y \equiv x^m \ mod\ p \\ y \equiv d_0^m \ mod\ p \end{cases}$$

e quindi

$$x^m \equiv d_0^m \ mod\ p,$$

allora esistono $0 \le i, j \le q-1$ tali che $x = \alpha^i$ e $d_0 = \alpha^j$. Pertanto, $\alpha^{im} \equiv \alpha^{jm} \ mod\ p$ e quindi $\alpha^{im} = \alpha^{jm}$ in $G \le \mathbb{Z}_p^*$ da cui segue che $q \mid m(i-j)$. Siccome $1 \le m \le q-1$ e q è primo, allora $q \mid (i-j)$ da cui segue che

$$x = \alpha^i = \alpha^j = d_0.$$

Siccome $d \not\equiv x^{e_1}\alpha^{e_2} \ mod\ p$ allora $x \not\equiv d^{1/e_1}\alpha^{-e_2/e_1} \ mod\ p$ e quindi $d_0 \not\equiv d^{1/e_1}\alpha^{-e_2/e_1} \ mod\ p$, ma ciò è assurdo essendo $d_0 = d^{1/e_1}\alpha^{-e_2/e_1}$. Pertanto, $\mathbf{P}[E_1 \cap E_2] = 0$ e quindi,

$$\mathbf{P}[E_1] = \mathbf{P}[E_1 \cap E_2] + \mathbf{P}[E_1 \cap E_2^c] = 0 + \mathbf{P}[E_1 \cap E_2^c] = \mathbf{P}[E_1 \cap E_2^c].$$

Dal **Teorema 13.23** segue che

$$\mathbf{P}[E_1] = \mathbf{P}[D\alpha^{-f_2} \equiv (d\alpha^{-e_2})^{f_1/e_1} \ mod\ p, y \not\equiv d_0^m \ mod\ p] = 1/q.$$

□

13.10 Firme fail-stop

Un **sistema di firma fail-stop** fornisce ulteriore sicurezza per prevenire la possibilità che un avversario avente infinite risorse computazionali sia in grado di falsificare una firma. Quando ciò si verifica, l'utente a cui è stata falsificata la firma è in grado di dimostrare l'avvenuta falsificazione.

In questo paragrafo finale, descriviamo il sistema di firma fail-stop costruito da **Pedersen-van Heyst** nel 1992.

Figura 13.4: Torben Pryds Pedersen e Pater Eugène van Heyst (1960)

Il sistema, come quello di Lamport è one-time e consiste di tre algoritmi:

- l'algoritmo di firma.
- l'algoritmo di verifica.
- l'algoritmo che dimostra l'avvenuta falsificazione.

Definizione 13.28. **(Sistema di Firma di Pedersen-van Heyst (1992))** Sia $p = 2q + 1$ un primo tale che q sia primo e che il PLD sia intrattabile in $\mathbb{Z}_p^*$. Siano α un elemento di ordine q in $\mathbb{Z}_p^*$, $1 \leq a_0 \leq q - 1$ e $\beta \equiv \alpha^{a_0} \ mod\ p$. La quadrupla $(p, q, \alpha, a_0, \beta)$ sono scelti da un ente di fiducia: (p, q, α, β) è pubblico, invece a_0 è privato (anche agli utenti). Siano $\mathcal{P} = \mathbb{Z}_q$, $\mathcal{A} = \mathbb{Z}_q \times \mathbb{Z}_q$ e la generica chiave è la sestupla

$$K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2),$$

dove $a_1, a_2, b_1, b_2 \in \mathbb{Z}_q$,

$$\begin{cases} \gamma_1 \equiv \alpha^{a_1}\beta^{a_2} \ mod\ p \\ \gamma_2 \equiv \alpha^{b_1}\beta^{b_2} \ mod\ p \end{cases} \tag{13.14}$$

con (γ_1, γ_2) pubblico e (a_1, a_2, b_1, b_2) privato.
Se $K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2)$ e x è un messaggio, allora

$$\text{sig}_K(x) = (a_1 + xb_1 \ mod\ q, a_2 + xb_2 \ mod\ q).$$

Se $(y_1, y_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$, allora

$$\text{ver}_K(x, y) = vero \iff \gamma_1\gamma_2^x \equiv \alpha^{y_1}\beta^{y_2} \ mod\ p.$$

Proposizione 13.29. Vale che

$$(y_1, y_2) = ((a_1 + xb_1) \ mod\ q, (a_2 + xb_2) \ mod\ q) \Rightarrow \gamma_1\gamma_2^x \equiv \alpha^{y_1}\beta^{y_2} mod\ p$$

Dimostrazione. Per (13.14) risulta

$$\begin{aligned} \gamma_1\gamma_2^x &\equiv (\alpha^{a_1}\beta^{a_2})\left(\alpha^{b_1}\beta^{b_2}\right)^x \ mod\ p \\ &\equiv \alpha^{a_1+xb_1}\beta^{a_2+xb_2} \ mod\ p \\ &= \alpha^{y_1}\beta^{y_2} \ mod\ p. \end{aligned}$$

□

Proposizione 13.30. Il sistema di firma di Pedersen-van Heyst è one-time.

Dimostrazione. Se $x \neq x'$ e

$$\begin{aligned} \text{sig}_K(x) &= (y_1, y_2) = ((a_1 + xb_1) \ mod\ q, (a_2 + xb_2) \ mod\ q) \\ \text{sig}_K(x') &= (y_1', y_2') = ((a_1 + x'b_1) \ mod\ q, (a_2 + x'b_2) \ mod\ q) \end{aligned}$$

allora

$$\begin{cases} y_1 = (a_1 + xb_1) \ mod\ q \\ y_2 = (a_2 + xb_2) \ mod\ q \\ y_1' = (a_1 + x'b_1) \ mod\ q \\ y_2' = (a_2 + x'b_2) \ mod\ q \end{cases}$$

Così

$$\begin{cases} a_1 = y_1 - x\,(y_1 - y_1')\,(x - x')^{-1} \mod q \\ b_1 = (y_1 - y_1')\,(x - x')^{-1} \mod q \\ a_2 = y_1' - x\,(y_1 - y_1')\,(x - x')^{-1} \mod q \\ b_2 = (y_2 - y_2')\,(x - x')^{-1} \mod q \end{cases}$$

e quindi $K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2)$ è nota, essendo $\gamma_1 \equiv \alpha^{a_1}\beta^{a_2} \mod p$ e $\gamma_2 \equiv \alpha^{b_1}\beta^{b_2} \mod p$.

□

Definizione 13.31. Siano $K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2)$ e $K' = (\gamma_1', \gamma_2', a_1', a_2', b_1', b_2')$ due chiavi nel sistema di firma di Pedersen-van Heyst, allora

$$K \sim K' \iff \gamma_1 = \gamma_1' \text{ e } \gamma_2 = \gamma_2'.$$

Quando ciò si verifca, diremo che K e K' sono equivalenti.

$\sim$ è una relazione di equivalenza sullo spazio delle chiavi $\mathcal{K}$.

Lemma 13.32. *Se $K \in \mathcal{K}$, allora $|[K]_\sim| = q^2$.*

Dimostrazione. Se $K, K' \in \mathcal{K}$ sono tali che $K \sim K'$, allora

$$K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2)$$
$$K' = (\gamma_1, \gamma_2, a_1', a_2', b_1', b_2').$$

Da (13.14) segue che

$$\begin{cases} \gamma_1 \equiv \alpha^{a_1}\beta^{a_2} \mod p \equiv \alpha^{a_1'}\beta^{a_2'} \mod p \\ \gamma_2 \equiv \alpha^{b_1}\beta^{b_2} \mod p \equiv \alpha^{b_1'}\beta^{b_2'} \mod p \end{cases}$$

Siccome $G = \langle\alpha\rangle$ e $\beta \equiv \alpha^{a_0} \mod p$ allora

$$\begin{cases} \alpha^{a_1 + a_0 a_2} \equiv \alpha^{a_1' + a_0 a_2'} \mod p \\ \alpha^{b_1 + a_0 b_2} \equiv \alpha^{b_1' + a_0 b_2'} \mod p \end{cases}$$

che è equivalente a

$$\begin{cases} a_1 + a_0 a_2 \equiv a_1' + a_0 a_2' \mod q \\ b_1 + a_0 b_2 \equiv b_1' + a_0 b_2' \mod q \end{cases}$$

essendo $o(\alpha) = q$. Pertanto

$$K \sim K' \iff K' = (\gamma_1, \gamma_2, a_1 + a_0 a_2 - a_0 a_2', a_2', b_1 + a_0 b_2 - a_0 b_2', b_2'),$$

con $a_2', b_2' \in \mathbb{Z}_q$. Quindi, $|[K]_\sim| = q^2$.

□

Lemma 13.33. *Se $K \sim K'$, allora*

$$\mathrm{ver}_K(x,y) = vero \iff \mathrm{ver}_{K'}(x,y) = vero.$$

Dimostrazione. Se $K, K' \in \mathcal{K}$ sono tali che $K \sim K'$, allora

$$K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2)$$
$$K' = (\gamma_1, \gamma_2, a_1', a_2', b_1', b_2')$$

e quindi

$$\begin{cases} \gamma_1 \equiv \alpha^{a_1}\beta^{a_2} \ mod\ p \equiv \alpha^{a_1'}\beta^{a_2'} \ mod\ p \\ \gamma_2 \equiv \alpha^{b_1}\beta^{b_2} \ mod\ p \equiv \alpha^{b_1'}\beta^{b_2'} \ mod\ p \end{cases}$$

Pertanto,

$$\mathrm{ver}_K(x,y) = vero \Leftrightarrow \gamma_1\gamma_2^x \equiv \alpha^{y_1}\beta^{y_2} \ mod\ p \Leftrightarrow \mathrm{ver}_{K'}(x,y) = vero.$$

□

Lemma 13.34. *Sia K una chiave e $y = \mathrm{sig}_K(x)$, allora esistono esattamente q chiavi K' tali che $K' \sim K$ e $y = \mathrm{sig}_{K'}(x)$.*

Dimostrazione. Determinare il numero delle chiavi $K' \sim K$ e $y = \mathrm{sig}_{K'}(x)$ equivale a determinare in corrispondenza della chiave pubblica (γ_1, γ_2) il numero delle quadruple (a_1, a_2, b_1, b_2) che sono soluzioni del sistema

$$\begin{cases} \gamma_1 \equiv \alpha^{a_1}\beta^{a_2} \ mod\ p \\ \gamma_2 \equiv \alpha^{b_1}\beta^{b_2} \ mod\ p \\ y_1 \equiv a_1 + xb_1 \ mod\ q \\ y_2 \equiv a_2 + xb_2 \ mod\ q. \end{cases} \tag{13.15}$$

Siccome, $G = \langle\alpha\rangle$, esistono (unici) $c_1, c_2, a_0 \in \mathbb{Z}_q$ tali che

$$\begin{cases} \gamma_1 \equiv \alpha^{c_1} \ mod\ p \\ \gamma_2 \equiv \alpha^{c_2} \ mod\ p \\ \beta \equiv \alpha^{a_0} \ mod\ p, \end{cases}$$

quindi (13.15) è equivalente a

$$\begin{cases} c_1 \equiv a_1 + a_0a_2 \ mod\ q \\ c_2 \equiv b_1 + a_0b_2 \ mod\ q \\ y_1 \equiv a_1 + xb_1 \ mod\ q \\ y_2 \equiv a_2 + xb_2 \ mod\ q. \end{cases} \tag{13.16}$$

che in notazione matriciale è

$$\begin{pmatrix} 1 & a_0 & 0 & 0 \\ 0 & 0 & 1 & a_0 \\ 1 & 0 & x & 0 \\ 0 & 1 & 0 & x \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ y_1 \\ y_2 \end{pmatrix} \tag{13.17}$$

Siccome K è una chiave che realizza $y = \text{sig}_K(x)$, allora il sistema (13.17) è compatibile. Se R_i denota l'i-sima riga della matrice del sistema (13.17), si ha che

$$R_1 + xR_2 - R_3 - a_0R_4 = O$$

e siccome R_1, R_2 e R_3 sono linearmente indipendenti, allora il rango della matrice del sistema (13.17) è 3. Il **Teorema di Rouché-Capelli** implica che (13.17) a coefficienti nel campo $\mathbb{Z}_q$ (q è primo) ammette $q^{4-3} = q$ soluzioni. Cioè q è il numero delle chiavi K' tali che $K' \sim K$ e $y = \text{sig}_{K'}(x)$.

□

Lemma 13.35. *Sia K una chiave e $y = \text{sig}_K(x)$. Se $\text{ver}_K(x', y') = vero$ con $x' \neq x$, allora esiste al più un'altra chiave K' tale che $K' \sim K$ e $y = \text{sig}_{K'}(x)$ e $y' = \text{sig}_{K'}(x')$.*

Dimostrazione. Determinare il numero delle chiavi $K' \sim K$ e $y = \text{sig}_{K'}(x)$ e $y' = \text{sig}_{K'}(x')$, sapendo che $\text{ver}_K(x', y') = vero$ con $x' \neq x$, equivale a determinare in corrispondenza della chiave pubblica (γ_1, γ_2) il numero delle quadruple (a_1, a_2, b_1, b_2) che sono soluzioni del sistema

$$\begin{cases} \gamma_1 \equiv \alpha^{a_1}\beta^{a_2} \ mod\ p \\ \gamma_2 \equiv \alpha^{b_1}\beta^{b_2} \ mod\ p \\ y_1 \equiv a_1 + xb_1 \ mod\ q \\ y_2 \equiv a_2 + xb_2 \ mod\ q \\ \gamma_1\gamma_2^{x'} = \alpha^{y_1'}\beta^{y_2'} \ mod\ p \\ y_1' \equiv a_1 + x'b_1 \ mod\ q \\ y_2' \equiv a_2 + x'b_2 \ mod\ q. \end{cases} \tag{13.18}$$

Poiché $y' = \text{sig}_{K'}(x')$, allora $\text{ver}_{K'}(x', y') = vero$. Dal **Lemma 13.33** segue che $\text{ver}_K(x', y') = vero$, quindi la quinta equazione del sistema (13.18) è sovrabbondante.
Siccome, $G = \langle\alpha\rangle$, esistono (unici) $c_1, c_2, a_0 \in \mathbb{Z}_q$ tali che

$$\begin{cases} \gamma_1 \equiv \alpha^{c_1} \ mod\ p \\ \gamma_2 \equiv \alpha^{c_2} \ mod\ p \\ \beta \equiv \alpha^{a_0} \ mod\ p, \end{cases}$$

quindi (13.18) è equivalente a

$$\begin{cases} c_1 \equiv a_1 + a_0a_2 \ mod\ q \\ c_2 \equiv b_1 + a_0b_2 \ mod\ q \\ y_1 \equiv a_1 + xb_1 \ mod\ q \\ y_2 \equiv a_2 + xb_2 \ mod\ q. \\ y_1' \equiv a_1 + x'b_1 \ mod\ q \\ y_2' \equiv a_2 + x'b_2 \ mod\ q. \end{cases} \tag{13.19}$$

che in notazione matriciale è

$$\begin{pmatrix} 1 & a_0 & 0 & 0 \\ 0 & 0 & 1 & a_0 \\ 1 & 0 & x & 0 \\ 0 & 1 & 0 & x \\ 1 & 0 & x' & 0 \\ 0 & 1 & 0 & x' \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ y_1 \\ y_2 \\ y_1' \\ y_2' \end{pmatrix} \tag{13.20}$$

Siccome $x \neq x'$, allora il rango della matrice del sistema è 4, per il **Teorema di Rouché-Capelli**, il sistema (13.20) è compatibile, ed in tal caso ammette un'unica soluzione se, e solo se, la matrice completa ha anche rango 4.

□

Teorema 13.36. *Se* $\text{sig}_K(x) = y$ *e* $x' \neq x$ *sono noti, allora la probabilità che un avversario calcoli* $\text{sig}_K(x')$ *è al più* $1/q$.

Dimostrazione. Se $\text{sig}_K(x) = y$ e $x' \neq x$ sono noti, per il **Lemma 13.34** ci sono esattamente q chiavi K' tali che $K' \sim K$ e $y = \text{sig}_{K'}(x)$ e, per il **Lemma 13.33**, al più una di esse è tale che $y' = \text{sig}_{K'}(x')$. Quindi, la probabilità che un avversario calcoli $y' = \text{sig}_{K'}(x')$ è al più $1/q$.

□

Il risultato contenuto nel **Teorema 13.36** non dipende dalle risorse computazionali dell'avversario, siccome quest'ultimo non riesce a dire quale delle q possibili chiavi è stata usata dall'utente firmatario. Pertanto, la sicurezza è incondizionata.

Analizziamo il concetto fail-stop. Supponiamo che ad un utente A gli venga fornita una coppia (x', y'') tale che

$$\begin{cases} \text{sig}_K(x') \neq y'' \\ \text{ver}_K(x', y'') = vero \end{cases}$$

cioè che

$$\begin{cases} \text{sig}_K(x') \neq y'' = (y_1'', y_2'') \\ \gamma_1 \gamma_2^{x'} \equiv \alpha^{y_1''} \beta^{y_2''} \ mod\ p \end{cases} \tag{13.21}$$

Allora l'utente A calcola la propria firma su x', quindi

$$\begin{cases} \text{sig}_K(x') = y' = (y_1', y_2') \\ \gamma_1 \gamma_2^{x'} \equiv \alpha^{y_1'} \beta^{y_2'} \ mod\ p. \end{cases} \tag{13.22}$$

Allora da (13.21) e (13.22), segue che

$$\alpha^{y_1''} \beta^{y_2''} \equiv \alpha^{y_1'} \beta^{y_2'} \ mod\ p.$$

Siccome $\beta \equiv \alpha^{a_0} \ mod\ p$, si ha

$$\alpha^{y_1'' + a_0 y_2''} \equiv \alpha^{y_1' + a_0 y_2'} \ mod\ p,$$

o equivalentemente

$$y_1'' + a_0 y_2'' \equiv y_1' + a_0 y_2' \ mod\ q \Longleftrightarrow y_1'' - y_1' \equiv a_0 (y_2' - y_2'') \ mod\ q \tag{13.23}$$

Siccome $y'' \neq y'$, da (13.23) segue che $y_1'' \neq y_1'$ e $y_2' \neq y_2''$. Pertanto, $y_2' - y_2''$ è invertibile in $\mathbb{Z}_q^*$ e quindi

$$a_0 = \log_\alpha \beta = (y_1'' - y_1')(y_2' - y_2'')^{-1} \ mod\ q \tag{13.24}$$

Siccome a_0 è noto solo all'ente di fiducia, poichè stiamo assumendo implicitamente che A non sia in grado di calcolare il logaritmo discreto $\log_\alpha \beta$. Quindi, il fatto che A sia in grado di determinare a_0 è una dimostrazione dell'avvenuta falsificazione.

Esempio 13.37. Sia $p = 3467 = 2 \times 1733 + 1$, e sia $\alpha = 4$ un elemento di ordine 1733 in $\mathbb{Z}_{3467}^*$. Sia $a_0 = 1567$, allora

$$\beta = 4^{1567} \ mod\ 3467 = 514.$$

Quindi, i valori scelti dall'ente di fiducia sono

$$(p, q, \alpha, a_0, \beta) = (3467, 1733, 4, 1567, 514),$$

i valori $(p, q, \alpha, \beta) = (3467, 1733, 4, 514)$ sono pubblici, invece $a_0 = 1567$ è segreto. Un utente A crea la sua firma usando $(a_1, a_2, b_1, b_2) = (888, 1024, 786, 999)$, quindi

$$\begin{aligned} \gamma_1 &= 4^{888} 514^{1024} \ mod\ 3467 = 3405 \\ \gamma_2 &= 4^{786} 514^{999} \ mod\ 3467 = 2281, \end{aligned}$$

$(\gamma_1, \gamma_2) = (3405, 2281)$ è pubblica, invece $(a_1, a_2, b_1, b_2) = (888, 1024, 786, 999)$ è privata.

Supponiamo che all'utente A sia inviato il messaggio $x = 3833$ munito di firma **falsificata** $(822, 55)$. La firma è valida perché la condizione di verifica è soddisfatta:

$$\begin{aligned} \gamma_1 \gamma_2^x &= 3405 \times 2281^{3833} \ mod\ 3467 = 2282 \\ \alpha^{y_1} \beta^{y_2} &= 4^{822} \times 514^{55} \ mod\ 3467 = 2282. \end{aligned}$$

Tuttavia, questa non è la firma che l'utente A avrebbe costruito.
Infatti, A produce la sua firma come segue:

$$\begin{aligned} a_1 + x b_1 \ mod\ q &= (888 + 3833 \times 786) \ mod\ 1733 = 1504 \\ a_2 + x b_2 \ mod\ q &= (1024 + 3833 \times 999) \ mod\ 1733 = 1291. \end{aligned}$$

Quindi la firma che A allega al messaggio $x = 3833$ è la coppia $(1504, 1291)$. Con queste informazioni, A calcola il logaritmo discreto con (13.24)

$$a_0 = \log_\alpha \beta = (8232 - 1504)(1291 - 55)^{-1} \ mod\ 1733 = 1567$$

che dovrebbe essere segreto. Questa è la prova dell'avvenuta falsificazione. Infatti, a_0 è noto solo all'ente di fiducia, siccome $a_0 = \log_\alpha \beta$ è computazionalemnte intrattabile.

□