SULLA PROBABILITA' DI INDOVINARE LA CHIAVE ED ALTERARE I MESSAGGI IN SISTEMI DI AUTENTICAZIONE BASATI SU PIANI PROIETTIVI FINITI[1]

Fernando Di Gennaro[2], Franco Eugeni[3], Antonio Maturo[4]

SUNTO – In questo lavoro vengono considerati sistemi di autenticazione basati su piani proiettivi finiti. Assumendo varie ipotesi per la distribuzione di probabilità a priori della chiave e sui criteri di scelta di un individuo *B* intenzionato a rompere il codice, si determinano, con considerazioni di tipo bayesiano, le probabilità di *B* di indovinare la chiave nei vari casi. Si considera anche un nuovo sistema di autenticazione basato sui nuovi concetti di metrica pseudoeuclidea e di perpendicolarità rispetto a tale metrica che assumono aspetti molto diversi a seconda che si considerino piani di ordine dispari o pari.

ABSTRACT – In this paper we consider some authentication systems based on projective finite planes. In various hypotheses on the "a priori" probability of key and on criteria of choice of an individual *B* that wants to break the code, we determine, by a Bayesian point of view, the probability of *B* to guess the key in the various cases. We consider also a new authentication system based on the new concepts of pseudo-Euclidean metric and perpendicularity as to such metrics, that are very different if the order of the plane is odd or even.

---

[1] Lavoro svolto nell'ambito della Ricerca MURST ex 40%, 1997-1998

[2] Università della Basilicata

[3] Università di Teramo

[4] Università di Chieti - Pescara

1. Sistemi di autenticazione su un piano proiettivo finito

Un sistema di autenticazione è basato su una funzione f di due variabili ed una chiave segreta K. La procedura è come segue:

a) un individuo S manda un messaggio M ed un autenticatore, che dipende da M e da K, $a = f(K, M)$;
b) un individuo R a cui sono stati inviati M ed a riceve un messaggio M' ed un autenticatore a'. Può essere che sia $M \neq M'$ oppure $a \neq a'$ per un difetto nel canale di trasmissione o per manomissione di una spia B;
c) R calcola $a'' = f(K, M')$. Se $a' = a''$ allora R considera il messaggio M' come originale, ossia valuta $M' = M$ altrimenti M è giudicato alterato.

Uno schema importante di autenticazione si ottiene considerando un piano proiettivo finito di ordine q, π_q. Si assume che i messaggi siano punti di una fissata retta r di π_q e le chiavi siano i punti di $\alpha_q = \pi_q - r$. Data una chiave K ed un messaggio M, si assume come autenticatore la retta passante per K e per M.
Nel caso desarguesiano i punti di π_q possono essere rappresentati con coordinate omogenee; risulta, per un opportuno numero naturale positivo n, $q = p^n$ con p numero primo, e, a meno di proiettività, si può sempre ritenere che la retta r sia la retta impropria.
Allora un messaggio M è un punto del tipo $(0, 1, m)$. Possiamo scrivere, in modo più sintetico, $M = [m]$. Una chiave K è un punto del tipo $(1, x_0, y_0)$ che indichiamo sinteticamente con $[x_0, y_0]$ e l'autenticatore è la retta che, in coordinate non omogenee, ha equazione:

$$y - y_0 = m\,(x - x_0). \qquad (1)$$

Noto il messaggio M e la chiave K, la retta a, per K e M, è individuata dalla coppia $(m, h = y_0 - m\,x_0)$. Noto m la retta è individuata solo dal numero h e scriviamo brevemente $a = [h]$.

2. Sulla probabilità di indovinare la chiave da un punto di vista bayesiano

Ci proponiamo di valutare le seguenti probabilità fra loro collegate:
1) *Probabilità che B trasmetta un autenticatore a' che sia uguale ad a'', ossia la probabilità che B riesca a fare accettare il messaggio alterato M'.*

2) Probabilità che B indovini la chiave.

Una trattazione generale del problema si ottiene utilizzando le *probabilità condizionate* e la *formula di Bayes.*
Indichiamo con I_K l'evento "*B indovina la chiave K*". Per poter calcolare la probabilità di I_K è necessario conoscere la distribuzione di probabilità "a priori" della chiave, ossia la funzione:

$$f: (x, y) \in \alpha_q \longrightarrow prob(K = [x, y]) \tag{2}$$

ed inoltre, per ogni punto $(x, y) \in \alpha_q$, la probabilità dell'evento condizionato:

$$I_K/[x, y] = \text{"}B \text{ indovina la chiave } K \text{ se } K = [x, y]\text{"}. \tag{3}$$

Ammettiamo, in questo lavoro, che per ogni punto $[x_0, y_0]$ del piano, ci sia sempre la possibilità (almeno dal punto di vista di S e di B) che sia $K = [x_0, y_0]$ anche se la probabilità di tale evento è nulla.
Per i teoremi delle probabilità totali e delle probabilità composte, indicando con $\pi(E)$ la probabilità di un evento E e con $\pi(E/H)$ quella di un evento condizionato E/H, si ha:

$$\pi(I_K) = \sum_{(x,y) \in \alpha_q} \pi(I_K \cap (K = [x, y]) = \sum_{(x,y) \in \alpha_q} \pi(I_K/[x, y])\, f(x, y). \tag{4}$$

Bisogna quindi valutare le probabilità a priori $f(x, y)$ che possono dipendere da motivi geometrici, statistici, dalle attitudini dell'individuo che assegna la chiave, etc., e le probabilità condizionate $\pi(I_K/[x, y])$ che dipendono dai criteri con cui l'individuo B effettua le sue scelte.
Vediamo alcuni casi.

I. B sceglie a caso senza informazioni

B non conosce la $f(x, y)$ o si comporta come se non la conoscesse, scegliendo a caso. Allora indica una chiave a caso fra tutti i punti del piano affine α_q, per cui risulta

$$\pi(I_K/[x, y]) = 1/q^2 = 1/p^{2n} \tag{5}$$

e quindi, poiché $\sum_{(x,y) \in \alpha_q} f(x, y) = 1$, segue

$$\pi(I_K) = 1/q^2 \sum_{(x,y) \in \alpha_q} f(x, y) = 1/q^2. \tag{6}$$

II. B sceglie conoscendo la funzione $f(x,y)$

Supponiamo che B conosca la funzione $f(x, y)$. Allora una buona strategia è quella di scegliere a caso uno dei punti in cui essa è massima.
Sia H l'insieme dei punti di α_p in cui la probabilità $f(x, y)$ è massima. Allora, se h è la cardinalità di H, si ha:

$$\pi(I_K/[x, y]) = \begin{cases} 0 & se\ (x, y) \notin H \\ \dfrac{1}{h} & se\ (x, y) \in H \end{cases} \quad (7)$$

Se $\mu(f)$ è il massimo valore assunto da f si ha:

$$\pi(I_K) = 1/h \sum_{(x,y) \in H} f(x, y) = h\, \mu(f)/h = \mu(f). \quad (8)$$

Risulta $1/q^2 \leq \mu(f) \leq 1/h$. L'uguaglianza a sinistra vale se la f è costante su tutto α_q e l'uguaglianza a d vale se la f è nulla in $\alpha_q - H$.
Quindi, se $f(x, y)$ è una costante, si riottiene la (6), in caso contrario si ha, per $\pi(I_K)$ un valore maggiore di $1/q^2$.
Ad esempio, se B conosce l'autenticatore a allora la funzione di probabilità $f(x, y)$ è nulla nei punti di $\alpha_q - a$. Se B è informato del fatto che la $f(x, y)$ è costante nei punti di a, si ha $\mu(f) = 1/q$ e dalla (8) segue la:

$$\pi(I_K) = 1/q. \quad (9)$$

III. B sceglie secondo una sua distribuzione di probabilità

L'individuo B decide di scegliere un punto $[x_0, y_0]$ secondo una sua distribuzione di probabilità. Ad esempio mette in un'urna, per ogni punto $[x, y]$, del piano affine α_q, palline contrassegnate con $[x, y]$ in numero proporzionale alla probabilità $\pi(I_K/[x, y])$ da lui attribuita. Successivamente estrae a caso una pallina dall'urna, legge il valore $[x, y]$ e sceglie tale punto come chiave. Poniamo:

$$\pi(I_K/[x, y]) = g(x, y). \quad (10)$$

Allora, per la (4), si ha:

$$\pi(I_K) = \sum_{(x,y) \in \alpha_q} f(x, y)\, g(x, y) \quad (11)$$

Ad esempio, B può porre $f(x, y) = g(x, y)$, $\forall (x, y) \in \alpha_q$. In tal caso si ha:

$$\pi(I_K) = \sum_{(x,y)\in\alpha_q} f^2(x, y) \qquad (12)$$

3. Confronto fra le probabilità ottenute

Interessante è il confronto fra le formule (6), (8) e (12) che ci permette di vedere come varia la probabilità di indovinare la chiave secondo i diversi comportamenti e le diverse conoscenze di S e di B.
A tale scopo indichiamo con $\pi^{(1)}(I_K)$, $\pi^{(2)}(I_K)$ e $\pi^{(3)}(I_K)$, rispettivamente, i valori di $\pi(I_K)$ dati dalle (6), (8) e (12). Si ha evidentemente: $\pi^{(1)}(I_K) \leq \pi^{(2)}(I_K)$ e l'uguaglianza vale se e solo se $f(x, y)$ è costante.
Inoltre, poiché la forma quadratica:

$$\sum_{i=1}^{N} x_i^2 \qquad (13)$$

con le condizioni:

$$\sum_{i=1}^{N} x_i = 1, \qquad x_i \geq 0, \quad \forall\, i \in \{1,2,.....,N\} \qquad (14)$$

è minima se e solo se $x_i = 1/N$, $\forall i \in \{1,2,\ldots,N\}$, si ha che $\pi^{(1)}(I_K) \leq \pi^{(3)}(I_K)$ e l'uguaglianza vale se e solo se $f(x, y)$ è costante.
Infine, poiché la forma quadratica (13), con le condizioni (14) è minore o uguale al massimo dei numeri $x_1, x_2, \ldots, x_N$, segue che $\pi^{(3)}(I_K) \leq \pi^{(2)}(I_K)$.

4. Sistema di autenticazione basato sullo pseudo prodotto interno

In [2] sono stati introdotti dei particolari prodotti scalari in $AG(2, q)$.
Siano $\mathbf{u} = (u_1, u_2)$, $\mathbf{v} = (v_1, v_2)$ due vettori di $AG(2, q)$ e sia θ un elemento di $GF(q)$ tale che, $\forall x \in GF(q)$, per q dispari sia $\theta \neq x^2$ e per q pari, sia $\theta \neq x^2+x$.

Per q dispari chiamiamo *pseudo prodotto scalare o interno* di $\mathbf{u}$ e $\mathbf{v}$, indicato con $\mathbf{u}\cdot\mathbf{v}$, l'elemento di $GF(q)$:

$$\mathbf{u}\cdot\mathbf{v} = u_1 v_1 - \theta\, u_2 v_2. \qquad (15)$$

Risulta $\mathbf{u}\cdot\mathbf{v} = \mathbf{v}\cdot\mathbf{u}$ e, poiché θ non è un quadrato, $\mathbf{u}\cdot\mathbf{u} = 0$ se e solo se $\mathbf{u} = \mathbf{0}$.

Per q pari definiamo i seguenti *pseudo prodotti scalari ordinati*:

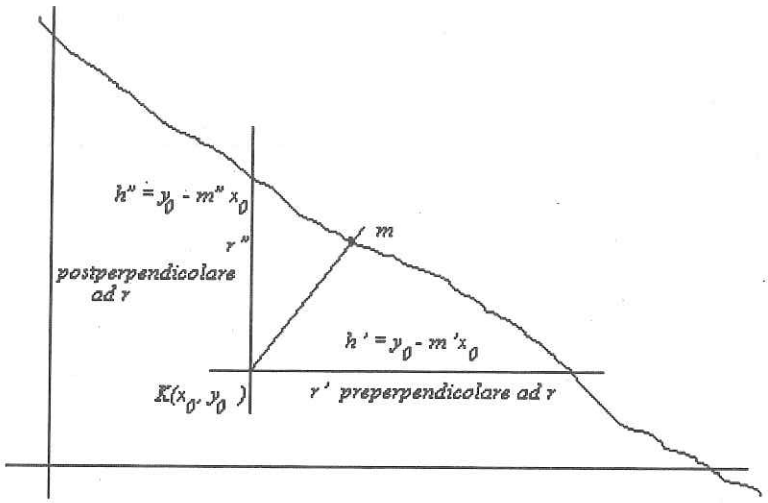
$$\mathbf{u}\cdot\mathbf{v} = u_1 v_1 + u_1 v_2 + \theta\, u_2 v_2, \qquad \mathbf{v}\cdot\mathbf{u} = u_1 v_1 + u_2 v_1 + \theta\, u_2 v_2 \qquad (16)$$

Risulta che $\mathbf{u}\cdot\mathbf{v} - \mathbf{v}\cdot\mathbf{u} = u_1 v_2 - u_2 v_1$ in generale è diverso da 0, per cui non vale, per q dispari, la proprietà commutativa dello pseudo prodotto scalare. Per $\mathbf{u} = \mathbf{v}$ si ha $\mathbf{u}\cdot\mathbf{u} = u_1^2 + u_1 u_2 + \theta u_2^2$ che, essendo $\forall x \in GF(q)$, $\theta \neq x^2 + x$, si annulla se e solo se $\mathbf{u} = \mathbf{0}$.

Nel caso dispari, fissato il vettore **u**, esiste, a meno di parallelismo e per la commutatività del prodotto scalare, un solo vettore **v** perpendicolare ad **u**.
Nel caso pari si possono definire, a meno di parallelismo e per la non commutatività del prodotto scalare, due vettori **v'** e **v''**, in generale non paralleli, perpendicolari ad **u**. Ci sembra comodo ed opportuno distinguere nominalmente queste due "perpendicolarità ordinate" nel modo che segue. Diciamo che **v'** è *pre-perpendicolare* ad **u** se si verifica che $\mathbf{v'}\cdot\mathbf{u} = 0$ e che **v''** è *post-perpendicolare* ad **u** se risulta che $\mathbf{u}\cdot\mathbf{v''} = 0$.

Segue che, nel caso dispari, data una retta r ed un punto P appartenente a $AG(2,q)$, esiste una ed una sola retta per P e perpendicolare alla retta r, mentre nel caso pari esistono due rette r' ed r'' passanti per P e perpendicolari ad r.
Precisamente poniamo:

- $r' \perp r$ se e solo se i vettori paralleli ad r' sono pre-perpendicolari a quelli paralleli ad r
- $r \perp r''$ se e solo se i vettori paralleli ad r'' sono post-perpendicolari a quelli paralleli ad r



I concetti di pre-perpendicolare e di post-perpendicolare permettono di ottenere nuovi sistemi di autenticazione dei messaggi. Precisamente, se $K = [x_0, y_0]$ è la chiave ed $M = [m]$ è il messaggio, si può inviare come autenticatore il numero: $h^* = y_0 - m^* x_0$ dove m^* è il coefficiente angolare della retta per K perpendicolare alla retta KM per q dispari e di una fra le rette pre-perpendicolare o post-perpendicolare per q pari.
Nel caso dispari la sostituzione dell'autenticatore $h = y_0 - m\ x_0$ con l'autenticatore h^* non modifica la probabilità di indovinare la chiave in quanto la cardinalità della retta per K ed M è uguale a quella della retta per K e con direzione perpendicolare a quella di M.
Nel caso pari invece, è possibile diminuire la probabilità che B indovini la chiave o faccia accettare un messaggio alterato.
Proponiamo una semplice procedura per ottenere ciò. Il mittente e il destinatario concordano, oltre alla chiave un numero z_0 uguale a 0 se si sceglie la pre-perpendicolare ed uguale ad 1 se si sceglie la post-perpendicolare. Di fatto la chiave K è sostituita dalla $K^* = [x_0, y_0, z_0]$ con l'aggiunta di un bit z_0.
Sia dunque q pari e indichiamo con m' ed m'', rispettivamente, i coefficienti angolari delle generiche rette pre-perpendicolari e post-perpendicolari alla KM. Poniamo $m^* = m' + z_0\,(m'' - m')$ ed assumiamo come autenticatore il numero $h^* = y_0 - m^* x_0$.
Se il mittente R invia il messaggio $M = [m]$ e l'autenticatore h^*, la spia B può calcolare m' ed m'' e sa che la chiave K si trova o sulla retta r' pre-perpendicolare ad M, di equazione $y = m' x + h^*$ oppure sulla retta r'' post-perpendicolare ad M, di equazione $y = m'' x + h^*$ ma non sa a quale delle due rette appartiene K. Se le due rette sono distinte la loro unione ha cardinalità $2q-1$,

maggiore della cardinalità q di r, per cui la probabilità che l'individuo B indovini la chiave è inferiore rispetto al sistema di autenticazione considerato nel primo paragrafo.
Mostriamo, di seguito, che le rette r' ed r'' sono sempre distinte.
Infatti, sia r la retta per K e per M. Supponiamo, per semplicità di calcolo, ciò che non lede la generalità, che M non sia il punto improprio di uno degli assi. Allora i vettori $\mathbf{u} = (1, m)$, $\mathbf{u'} = (1, m')$ ed $\mathbf{u''} = (1, m'')$ sono, rispettivamente, paralleli ad r, r' ed r''. Si hanno allora le seguenti relazioni:

$$1 + m + \theta m m' = 0; \qquad 1 + m'' + \theta m m'' = 0. \tag{17}$$

Dalle (17) si ricavano le

$$m' = (1 + m)/(\theta m); \qquad m'' = 1/(1 + \theta m)$$

per cui i vettori $\mathbf{u'}$ ed $\mathbf{u''}$ sono coincidenti se e solo se

$$\theta m^2 + m + 1 = 0. \tag{18}$$

La (18) equivale a porre $\theta = (1/m) + (1/m)^2$ e, poiché $\theta \neq x + x^2$, $\forall x \in GF(q)$, essa non ammette soluzioni. Allora è sempre $m' \neq m''$ per cui ogni pre-perpendicolare r' ad r ed ogni post-perpendicolare r'' sono sempre distinte.

Se $f(x,y)$ è la distribuzione di probabilità "a priori" della chiave, risulta che $f(x,y) = 0$ per $(x,y) \notin r' \cup r''$ e vale la formula (8) con $H \subseteq r' \cup r'$. Se, come in genere si ammette, B è informato che la f(x,y) è costante in $r' \cup r'$ allora dalla (8) si ottiene la

$$\pi(I_K) = 1/(2q-1). \tag{19}$$

In tali ipotesi appare rilevante il confronto fra la formula (9) che ci dà la probabilità di indovinare la chiave negli usuali sistemi di autenticazione, e la (19) che mostra come tale probabilità si riduce del fattore (2-1/q) e quindi è praticamente la metà del caso classico.

5. Conclusioni ed applicazioni

Nella pratica un messaggio autenticato è del tipo $m_1 m_2 \ldots m_i a m_{i+1} \ldots m_n$ dove a è l'autenticatore ed $m_1 m_2 \ldots m_i m_{i+1} \ldots m_n$ il messaggio. Le m_i, $i = 1, 2, \ldots, n$, sono successioni di bit di uguale lunghezza n, ad esempio 64 bit, e rappresentano le parti in cui è diviso il messaggio. L'autenticatore si può trovare prima di m_1 o

dopo una qualsiasi delle m_i. Spesso è conveniente che l'autenticatore a non abbia la stessa lunghezza del messaggio, ma lunghezza uguale ad una delle sue parti m_i. In tal caso per autenticare l'intero messaggio si può procedere con una formula ricorrente nella maniera seguente.
Sia $t = f(x, y, z)$ una funzione definita in $(GF(2^n))^3$ ed a valori in $GF(2^n)$, tale che, fissati x, y e t, esista un solo valore di z tale che $t = f(x, y, z)$.
Sia $K = [x_0, y_0]$ la chiave e poniamo $a_0 = 0$. Per ogni $i \in \{1, 2, \ldots, n\}$, autentichiamo il messaggio parziale m_i con l'autenticatore

$$a_i = f(x_0, y_0, m_i + a_{i-1}). \tag{20}$$

L'autenticatore finale a_n si indica con a e si assume come autenticatore dell'intero messaggio.
Nel sistema di autenticazione considerato nel primo paragrafo si assume

$$t = f(x, y, z) = y - z\,x, \text{ da cui } a_i = y_0 - (m_i + a_{i-1})\,x_0. \tag{21}$$

Nel sistema di autenticazione considerato nel paragrafo 4 si assume invece

$$t = f(x, y, z) = y - z^*\,x, \text{ con } z^* = z' + b\,(z'' - z') \tag{22}$$

dove b può assumere solo valore 0 o 1, z è interpretato come un coefficiente angolare e z' e z'' sono i coefficienti angolari delle direzioni rispettivamente pre-perpendicolare e post-perpendicolare a z. Risulta quindi

$$a_i = y_0 - ((m'_i + b\,(m''_i - m'_i))\,a_{i-1})\,x_0. \tag{23}$$

Una ulteriore sicurezza nel processo di autenticazione dei messaggi si può ottenere utilizzando un funzione "*unidirezionale*" ossia una biiezione $v = g(u)$ definita in $GF(2^n)$ ed a valori in $GF(2^n)$ tale che, dato u, si possa calcolare agevolmente v, mentre, dato v, sia praticamente impossibile calcolare v a meno di non conoscere una opportuna chiave K^*.
In tal caso, si può sostituire l'autenticatore a con $g(a)$ e solo chi conosce K^* può risalire da $g(a)$ ad a.
La formula ricorrente (20) può allora essere sostituita dalla

$$a_i = f(x_0, y_0, m_i + g(a_{i-1})). \tag{24}$$

L'autenticatore finale inviato è $g(a_n)$.

BIBLIOGRAFIA

1 A. BEUTELSPACHER, *Criptology*, Mathematical Association of America, (1994)

2 F. DI GENNARO, F. EUGENI, *Strutture pseudo-euclidee su campi di Galois.* Le Matematiche, vol. LII (1997)- Fasc. I, pp.129-142.

3 F. EUGENI, A. MATURO, *Generalized Affine Planes.* Journal of Information & Optimization Sciences, vol.12 (1991), No.3, pp. 431–439.

4 F. EUGENI, A. MATURO. *A New Authentication System Based on the Generalized Affine Planes.* Journal of Information & Optimization Sciences, vol.13 (1992), No.2, pp.183–193.

6 F. EUGENI, A. MATURO, *Piani Affini su Anelli Finiti.* Atti del Convegno Nazionale Mathesis (1990), Iseo, pp 152-161

7 F. EUGENI, *Combinatorics and Criptography*, Annals of Discrete Mathematics, **52**, (1990), pp. 159 – 174

8 R. SCOZZAFAVA, *La probabilità soggettiva e le sue applicazioni,* Masson (1997).

9 A. SGARRO, *Crittografia*, Franco Muzzio Editore, (1993), pp. 94-96