NEURAL NETWORKS AND THEIR CRYPTOGRAPHIC APPLICATIONS

David POINTCHEVAL

Laboratoire d'Informatique
École Normale Supérieure

THE PROBLEM

The Perceptrons Problem **PP**

- Given: an ε-matrix A of size $m \times n$
- Find: an ε-vector V of size n such that

$$AV \geq 0$$

- **NP**-complete $\Rightarrow$ difficult to solve
- Max-**SNP**-hard $\Rightarrow$ difficult to approximate

The Permuted Perceptrons Problem **PPP**

- Given: an ε-matrix A of size $m \times n$
  and a multiset S of integers, of size m
- Find: an ε-vector V of size n such that

$$\{\{(AV)_j | j = \{1, \ldots, m\}\}\} = S$$

Finite field

$$\|T\|_\infty \leq t$$

if n is an odd nonnegative integer

$$2p > n + t$$

then $AY = T \Leftrightarrow AY = T \bmod p$

SIZE OF THE PROBLEM

Only one solution

- $N(m,n)$, number of solutions for an average instance of **PP**.
- $P_{m,n,S}$, probability to obtain a given multiset S with the product.

We want $N(m,n) \times P_{m,n,S} \leq 1$ for every multiset S.

Approximatively, $n \approx m + 16$ for all $100 < m < 200$.

m	n
101	117
121	137
141	157

$\Rightarrow$ the average number of solutions is between 0.9 and 1.1

Attacks

- no algebraic structure $\longrightarrow$ no Gaussian elimination
  $\longrightarrow$ apparently, only exhaustive or probabilistic attacks
- simulated annealing: the most efficient algorithm

size	#solutions **PP**	workload for Pr=$\frac{1}{2}$
101×117	$4.7\ 10^9$	2^{64}
121×137	$8.7\ 10^{10}$	2^{68}
151×167	$3.7\ 10^{12}$	2^{74}

Suggested size

Then, we can suggest:

$m = 101$, $n = 117$, $p = 127$ and $t = 33$

PROTOCOLS

Initialization

- common data:
  - m, n, p and t s.t. $2p > t + n$
  - h, a collision-free random hash function
  - M, a random ε-matrix of size $m \times n$
- secret key: an ε-vector V of size n
- public key:
  - the ε-vector L of size m s.t. $\text{Diag}(L)MV \geq 0$
  - the multiset $S = \{\{L_j(MV)_j | j = \{1, \ldots, m\}\}\}$

  then the problem associated to this user is $(A = \text{Diag}(L)M,\ S)$

For each identification, the prover

- selects:
  $P \in S_{m-1}$, $Q \in S^{\pm}_{n-1}$
  $W \in \mathbb{Z}(p)^n$
- computes:
  $A' = PAQ$, $V' = Q^{-1}V$

The Three Pass Identification Protocol (3p zk)

Prover		Verifier
$R = W + V'$, $h_0 = h(P\|Q)$, $h_1 = h(W)$, $h_2 = h(R)$, $h_3 = h(A'W)$, $h_4 = h(A'R)$		
	$\xrightarrow{h_0, h_1, h_2, h_3, h_4}$	
	$\xleftarrow{c}$	$c \in_R \{0, 1, 2, 3\}$
If $c = 0$	$\xrightarrow{P, Q, W}$	Checks h_0, h_1 and h_3
If $c = 1$	$\xrightarrow{P, Q, R}$	Checks h_0, h_2 and h_4
If $c = 2$	$\xrightarrow{A'W, A'V'}$	Checks $A'V'$, h_3 and h_4
If $c = 3$	$\xrightarrow{W, V'}$	Checks V', h_1 and h_2

The Five Pass Identification Protocol (5p zk)

Prover		Verifier
$h_0 = h(P\|Q)$, $h_1 = h(W\|V')$, $h_2 = h(A'W\|A'V')$		
	$\xrightarrow{h_0, h_1, h_2}$	
	$\xleftarrow{k}$	$k \in_R \mathbb{Z}^\star(p)$
$R = kW + V'$, $h_3 = h(R)$, $h_4 = h(A'R)$		
	$\xrightarrow{h_3, h_4}$	
	$\xleftarrow{c}$	$c \in_R \{0, 1, 2\}$
If $c = 0$	$\xrightarrow{P, Q, R}$	Checks h_0, h_3 and h_4
If $c = 1$	$\xrightarrow{A'W, A'V'}$	Checks $A'V'$, h_2 and h_4
If $c = 2$	$\xrightarrow{W, V'}$	Checks V', h_1 and h_3

RESULTS

Properties

Both protocols are

- some Interactive Proof System for **PPP**
  The probability for a cheater to be accepted is less than
  - $(\frac{3}{4})^r$ after r rounds with 3p zk
  - $(\frac{2p-1}{3(p-1)})^r$ after r rounds with 5p zk
- *zero-knowledge*

Light versions exist, but they are no longer *zero-knowledge*.

Performances

	SD Stern	SD Vron	CLE Stern	PKP Shamir	PPP 3p ZK	PPP 5p ZK
matrix size	256×512		24×24	37×64	101×117	
over the field	$\mathbb{F}_2$		$\mathbb{F}_{16}$	$\mathbb{F}_{251}$	$\mathbb{F}_2$	
best known attack complexity	2^{68}		2^{52}	2^{142}	2^{64}	
Number of rounds	35	35	20	20	48	35
public key (bits)	256	256	80	296	144	
secret key (bits)	512	512	80	384	117	
bits sent by round	954	47740	824	832	896	1040
global transmission rate (kbytes)	4.08	204	2.01	2.03	5.25	4.44

Conclusion

- few data must be communicated
- very short keys
- only very simple operations:
  additions and subtractions over small integers
- little RAM
- little EEPROM

$\Downarrow$

Well suited for smart card applications