A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis

30/08/2005

J.S. Coron, G. Poupard and D. Lefranc

(Unrestricted)

Overview

- Introduction : the GPS scheme
- A new type of private keys for GPS [CHES'04]
  - Description
  - Cryptanalysis
- First improvement of cryptanalysis
- Second improvement of cryptanalysis
- Conclusion

Introduction : the GPS scheme

Introduction : the GPS scheme (1)

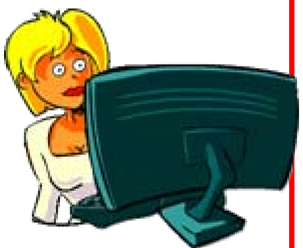
- The scheme
  - Introduced by Girault in 1991
  - Proved secure by Poupard and Stern in 1998

- Parameters/keys
  - Public key
    - n a RSA modulus
    - g an invertible element in $(Z/nZ)^*$
    - v an element of $<g>$; *i.e.* $v = g^{-s} \bmod n$
  - Private key
    - s *in* $[0, \mathrm{ord}(g)[$

Introduction : the GPS scheme (2)

$v = g^{-s} \bmod n$

Off-line computation



$$r \in [0, 2^R[$$

$$W = g^r \bmod n$$

$\xrightarrow{W}$

$\xleftarrow{c}$ $\quad c \in [0, 2^k[$

$$y = r + sc$$

$\xrightarrow{y}$

On-line computation

$$g^y v^c = W \bmod n$$

Introduction : the GPS scheme (3)

- If used with the precomputation of $W=g^r \bmod n$
  - Very efficient scheme for the prover : only $y=r+sc$
  - Eventually in RFID tags
    - few computation capabilities
      - *Improvement of GPS for a better integration?*

At CHES'04, Girault and Lefranc suggested 3 improvements : one is a new type of private keys

A new type of private keys for GPS

New private keys for GPS : description (1)

- The new type of private keys :
  - *$s=s_1s_2$ with s_1 in X_1 and s_2 in X_2*
    - s_1 and s_2 with a low Hamming weight
    - the computation of $s \times c$ is improved

New private keys for GPS : security (1)

The new type of private keys: *$s=s_1s_2$ with s_1 in X_1 and s_2 in X_2*

- Security?
  - <u>In a group of known order q</u>

$$v = g^{s_1 s_2 \bmod q} \bmod p \Rightarrow v^{s_1^{-1} \bmod q} \bmod p = g^{s_2} \bmod p$$

- With a BSGS-like algorithm : recovers the key in *$O(|X_1|+|X_2|)$ group exp.*

  - GPS : group order is unknown. This attack is not possible

New private keys for GPS : security (2)

The new private key: *$s = s_1 s_2$ with s_1 in X_1 and s_2 in X_2*

- Security?
  - GPS uses a RSA modulus
    - *ord(g)* unknown to the enemy
    - s_1^{-1} *mod ord(g)* infeasible
    - No better known attack than an exhaustive search In time *$O(\ |X_1| \times |X_2|\ )$ group exp.*
  - *Note :Stinson's attack for low Hamming weight private keys*

New private keys for GPS : security (3)

- we present here two new algorithms to better the cryptanalysis of such private keys
  - One general improvement for product in groups of unknown order
  - One specific improvement for such private keys

First improvement of cryptanalysis

First improvement of cryptanalysis (1)

- Basic idea :

$$v = g^{s_1 s_2 \bmod q} \bmod p \Rightarrow v^{s_1^{-1} \bmod q} \bmod p = g^{s_2} \bmod p$$

Inverting is infeasible, but :

$$\left(v^{s_1^{-1} \bmod q}\right)^{\prod_{j \in X_1} j} = \left(g^{s_2}\right)^{\prod_{j \in X_1} j}$$

$$\Leftrightarrow v^{\prod_{j \in X_1 \setminus \{s_1\}} j} = \left(g^{\prod_{j \in X_1} j}\right)^{s_2}$$

- BSGS-like algorithm can be performed

First improvement of cryptanalysis (2)

- BSGS algorithm $$v^{\prod_{j\in X_1\backslash\{s_1\}} j} = \left(g^{\prod_{j\in X_1} j} \right)^{s_2}$$
  - 2 sets :

$$\left\{ v^{\prod_{j\in X_1\backslash\{a\}} j}, a \in X_1 \right\} \qquad \left\{ \left(g^{\prod_{j\in X_1} j} \right)^{b}, b \in X_2 \right\}$$

- Search a same element for a given *a* and *b*
  - The private key is equal to *a*x*b*

First improvement of cryptanalysis (3)

- Complexity?
  - Computation of $\left\{ v^{\prod_{j \in X_1 \setminus \{a\}} j}, a \in X_1 \right\}$?
    - With a basic method, in time $O(|X_1|^2)$ group exp.
  - Computation of $\left\{ \left(g^{\prod_{j \in X_1} j} \right)^b, b \in X_2 \right\}$?
    - Once $g^{\prod_{j \in X_1} j}$ is computed : in time $O(|X_2|)$ group exp.

First improvement of cryptanalysis (4)

- The computation of $\left\{ v^{\prod_{j \in X_1 \setminus \{a\}} j}, a \in X_1 \right\}$ in time $O(|X_1|^2)$ group exp. must be improved

  - Otherwise :
    - the BSGS algorithm in time $O(|X_1|^2+|X_2|)$ group exp.
    - An exhaustive search in time $O(|X_1| \times |X_2|)$ group exp.

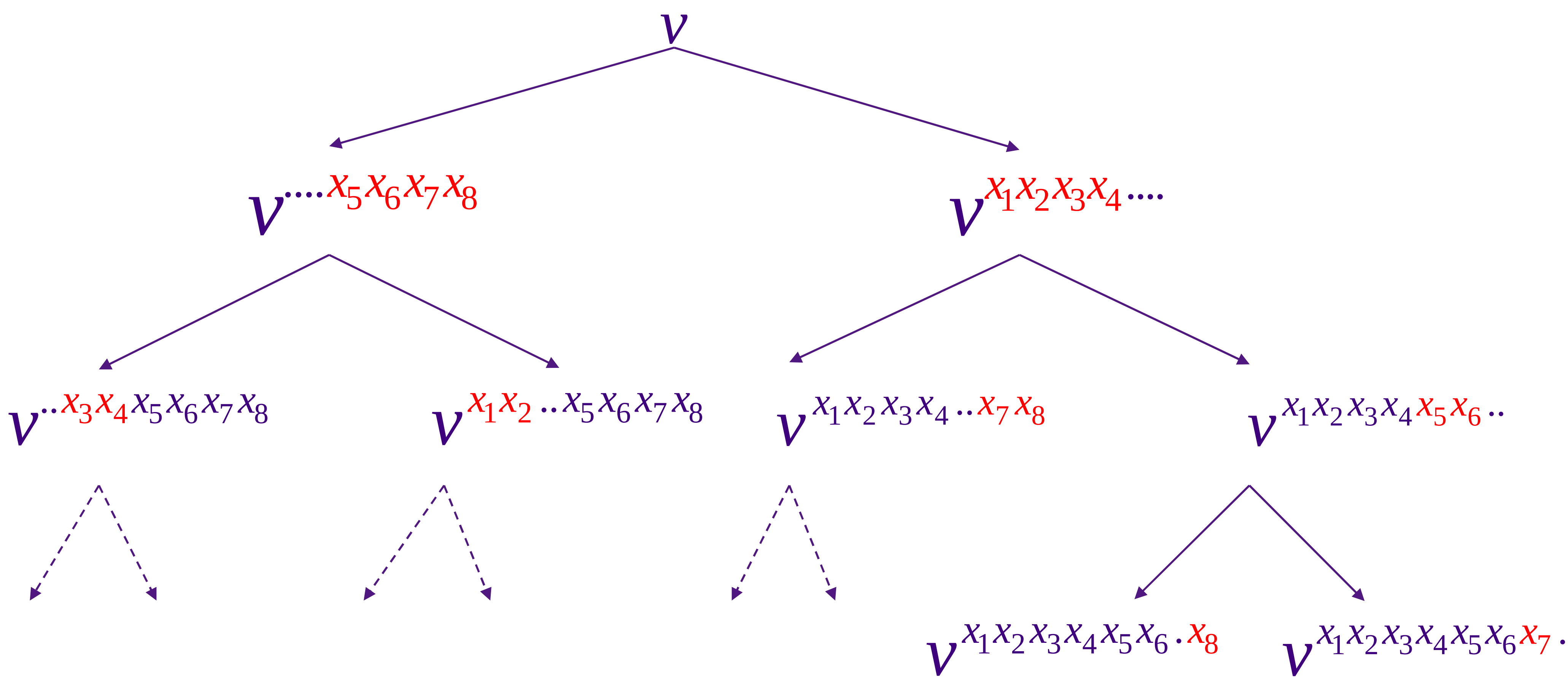
Not a better cryptanalysis!

We present a new method in time $O\big(|X_1| ln(|X_1|)\big)$ group exp.

First improvement of cryptanalysis (5)

- The trick for an efficient computation :
  - Use of a binary tree structure
    - The tree does not need to be saved
  - Description for a set $X = \{x_1, x_2, \ldots, x_8\}$ of cardinality $8 = 2^3$

First improvement of cryptanalysis (5)



First improvement of cryptanalysis (6)

- Analysis of the algorithm :
  - *Depth of the tree : $\ln |X|$*
  - Each step involves exactly $|X|$ group exp.

    Time complexity : $O(|X| \ln |X|)$ group exp.

First improvement of cryptanalysis (7)

- Complexity of the full BSGS-like algorithm :

  $O(|X_2|+|X_1| \ln |X_1|)$ *group exp.*

  - *In comparison with the exhaustive search in*

    $O(|X_2| \times |X_1|)$ *group exp.*

First improvement of cryptanalysis (8)

- Numerical application
  - s_2 a 142-bit number with 17 non-zero bits
  - s_1 a 19-bit number with 6 non-zero bits
    - Exhaustive search in 2^{80} group exp.
    - With the new BSGS-like algorithm :

      in time 2^{69} group exp.

Second improvement of cryptanalysis

Second improvement of cryptanalysis (1)

- The new private key: *$s=s_1s_2$ with s_1 in X_1 and s_2 in X_2*
  - s_1 and s_2 with a low Hamming weight

$$v = g^{s_1 s_2} \Leftrightarrow v = \left(g^{s_1}\right)^{s_2} = h^{s_2}$$

  - in base *h*, *v* has a low hamming weight
    - Stinson attack can be applied for each possible *h*

Second improvement of cryptanalysis (2)

- Numerical application

  - s_2 a 142-bit number with 17 non-zero bits
  - s_1 a 19-bit number with 6 non-zero bits

    - Exhaustive search in 2^{80} group exp.
    - With the new BSGS-like algorithm : 2^{69} group exp.

    - The new attack : 2^{54} group exp.

Conclusion

- 2 improvements of cryptanalysis for new GPS private keys
  - One is a new BSGS algorithm for product in group of unknown order
    - Almost the same complexity as in groups of known order
  - One specific to the new private keys.