Example for BSGS

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

The BSGS algorithm – example

Baby steps

- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation

- Reach g^m, invert: $S = g^{-m}$.

Giant steps

- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus
$S \equiv 22^{-1} \equiv 41 \bmod 53$.

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus $S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$							

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus $S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33						

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus $S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33	28					

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus $S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33	28	35				

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus
$S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33	28	35	4			

We have a match at $i = 2, j = 3$

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus
$S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33	28	35	4			

We have a match at $i = 2, j = 3$

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus
$S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33	28	35	4			

We have a match at $i = 2, j = 3$

Thus $a = i + jm = 2 + 3 \cdot 7 =$

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus $S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33	28	35	4			

We have a match at $i = 2, j = 3$

Thus $a = i + jm = 2 + 3 \cdot 7 = 23$.

The BSGS algorithm – example

Baby steps
- Compute table with (g^i, i) for $0 \leq i < m$;
- Sort by first element while computing.

Preparation
- Reach g^m, invert: $S = g^{-m}$.

Giant steps
- Starting at $j = 0, 1, 2, 3, \ldots$,
  compute $S^j h$ and compare with table entries.
  Match instantly gives $g^{-jm} h = g^i$,
  thus $a = i + jm$.

$G = \mathbb{F}_{53}^*$, generated by $g = 2$. $m = \lfloor \sqrt{52} \rfloor = 7$. Target $h = 33$.

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	32	11

$2^7 = 2 \cdot 11 = 22$. Thus $S \equiv 22^{-1} \equiv 41 \bmod 53$.

For calculations by hand we skip the sorting part.

j	0	1	2	3	4	5	6
$S^j h$	33	28	35	4			

We have a match at $i = 2, j = 3$

Thus $a = i + jm = 2 + 3 \cdot 7 = 23$. Verify $2^{23} \equiv 33 \bmod 53$.