New Scalar Multiplication Speed Record

Chitchanok Chuengsatiansup

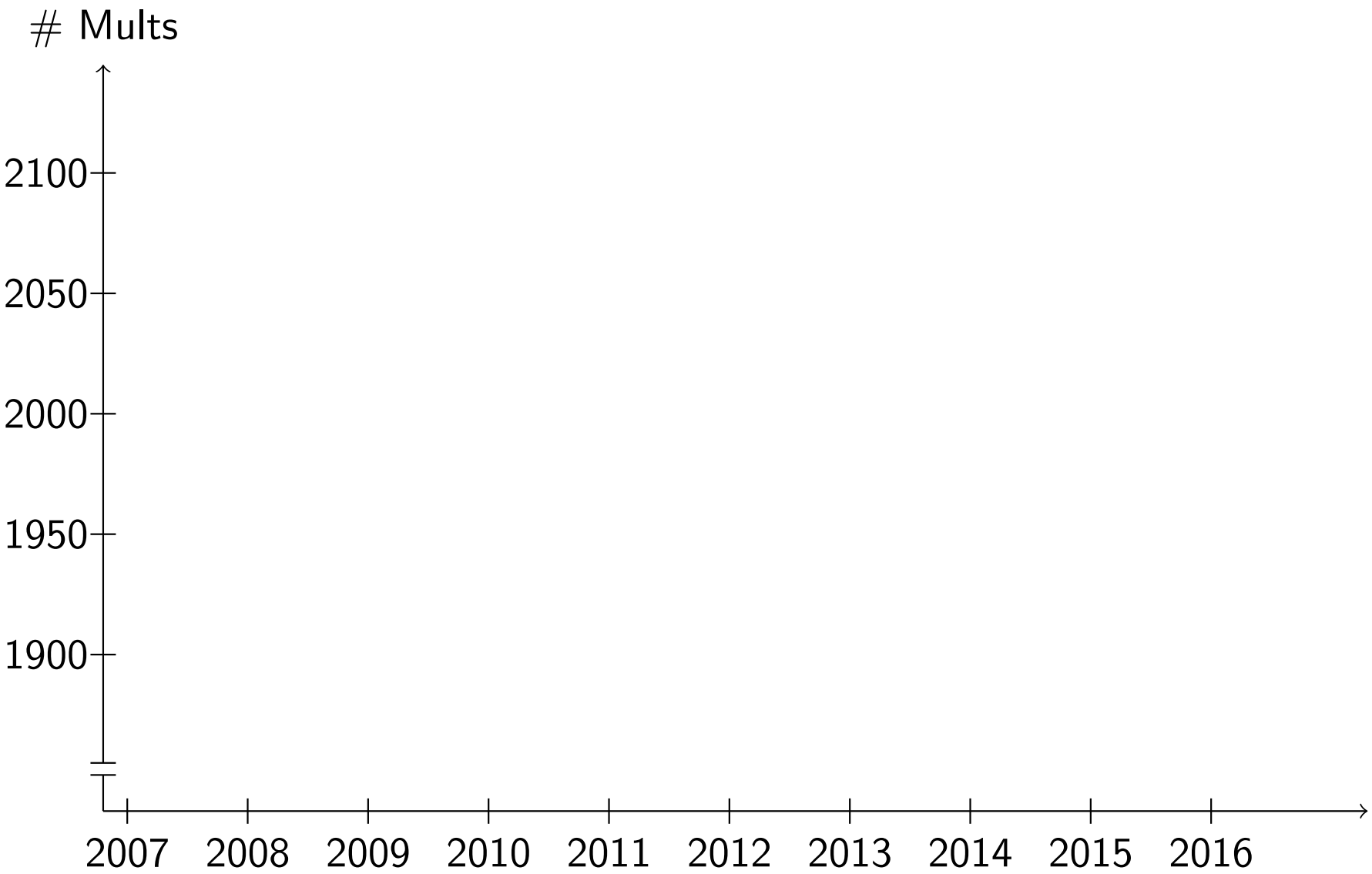
Technische Universiteit Eindhoven

September 28, 2015

Joint work with Daniel J. Bernstein and Tanja Lange

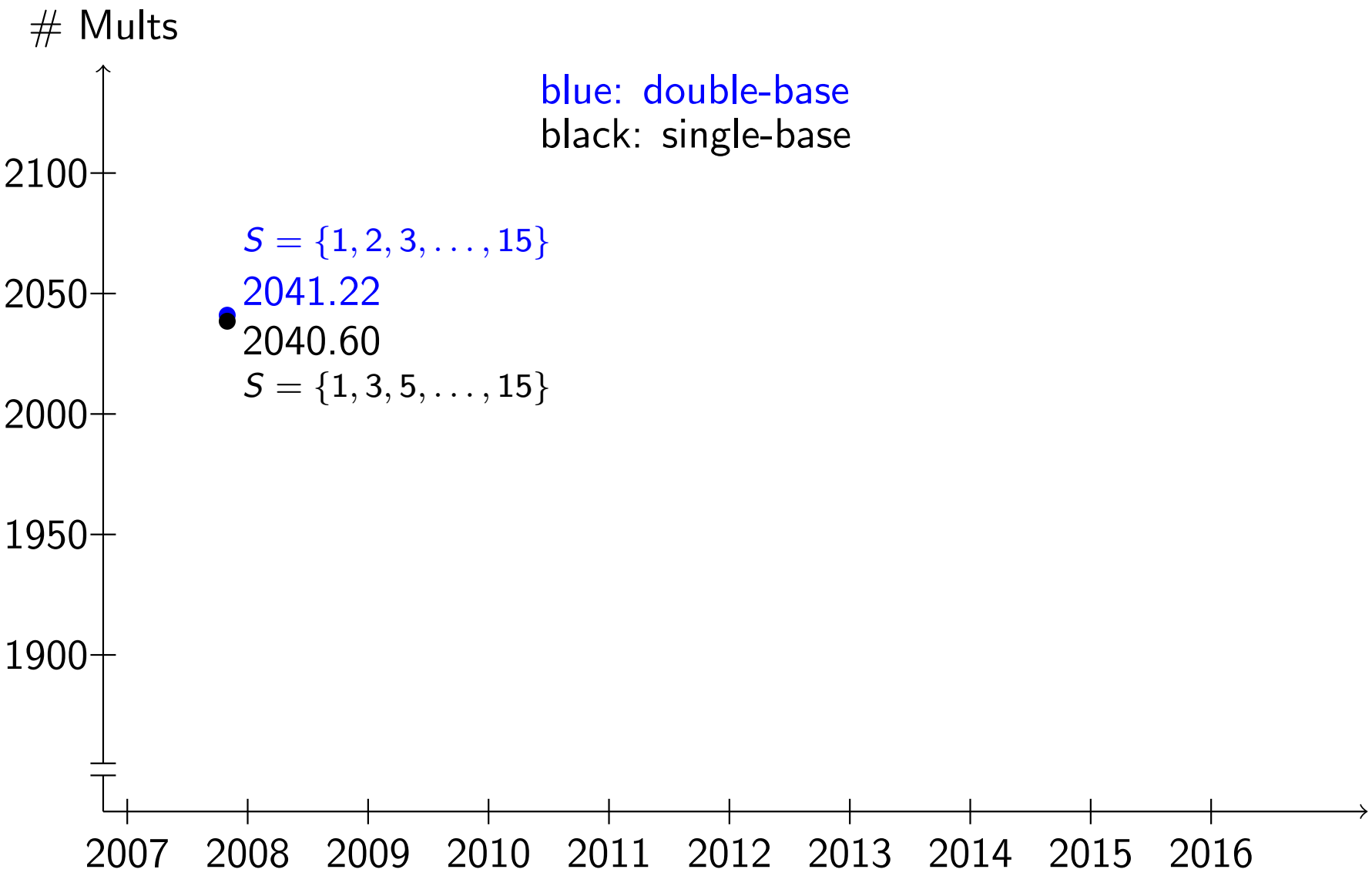
Single- VS Double-base

Scalar multiplication for 256-bit integer on Edwards curve



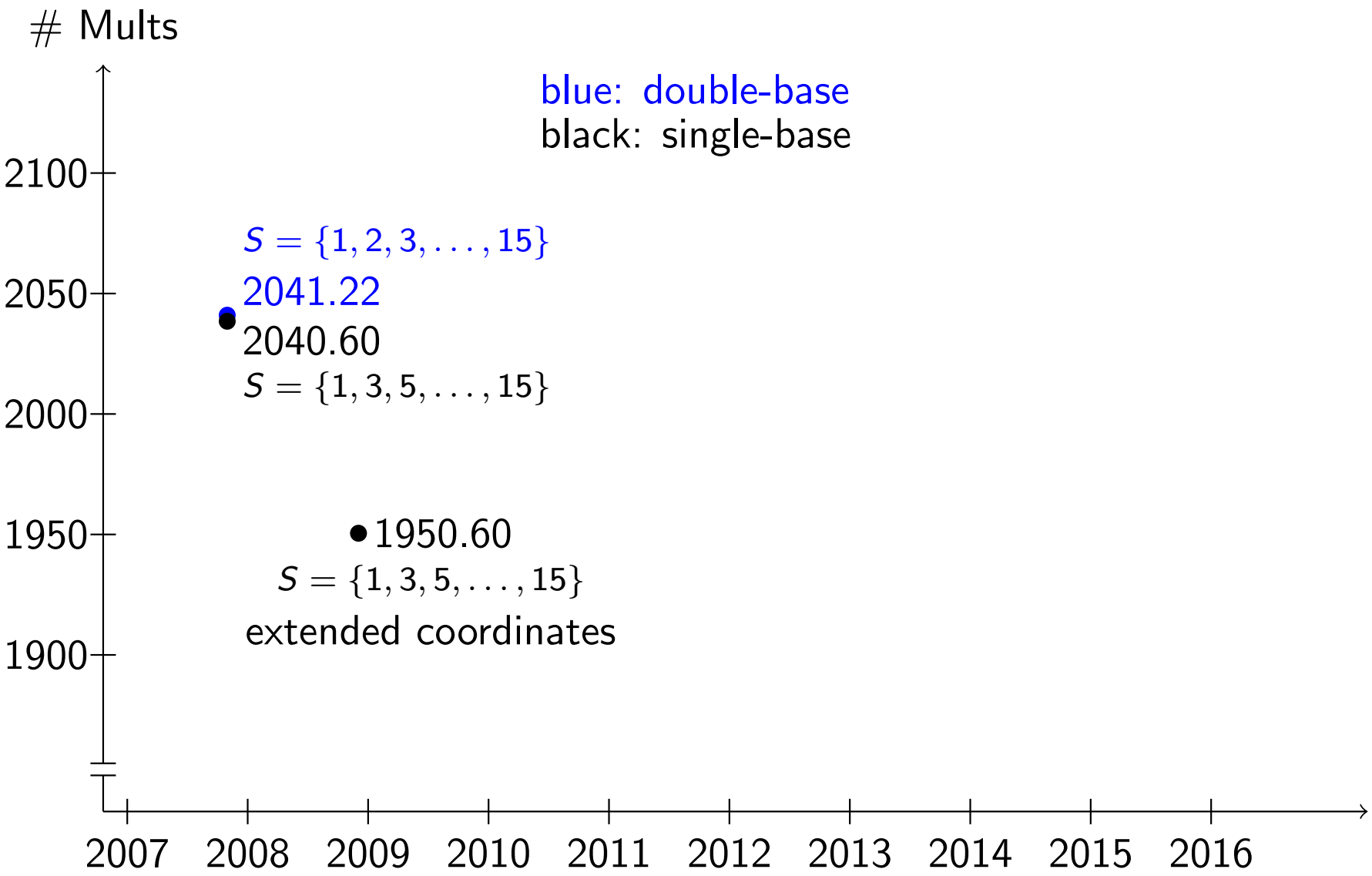
Single- VS Double-base

Scalar multiplication for 256-bit integer on Edwards curve



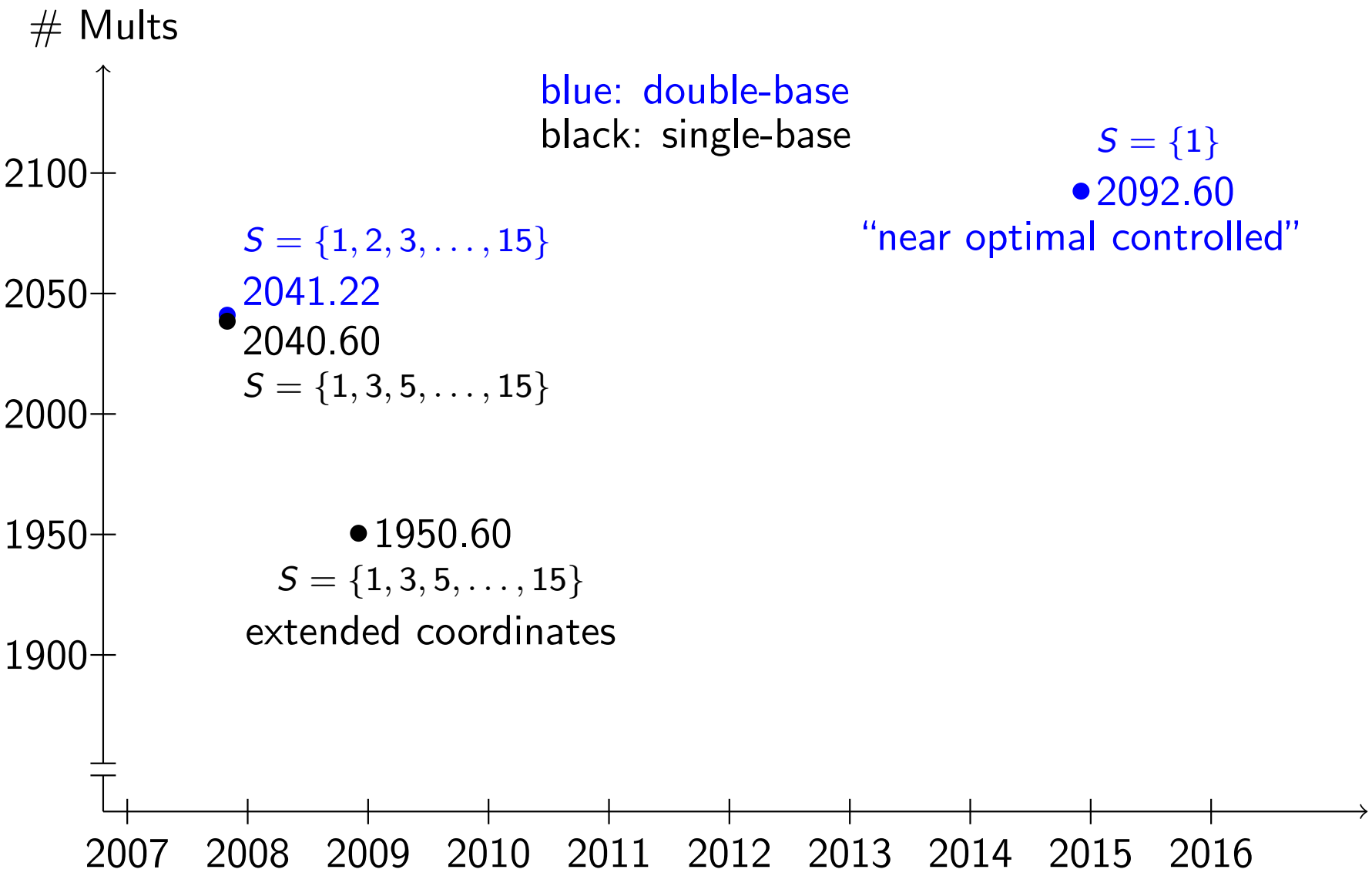
Single- VS Double-base

Scalar multiplication for 256-bit integer on Edwards curve



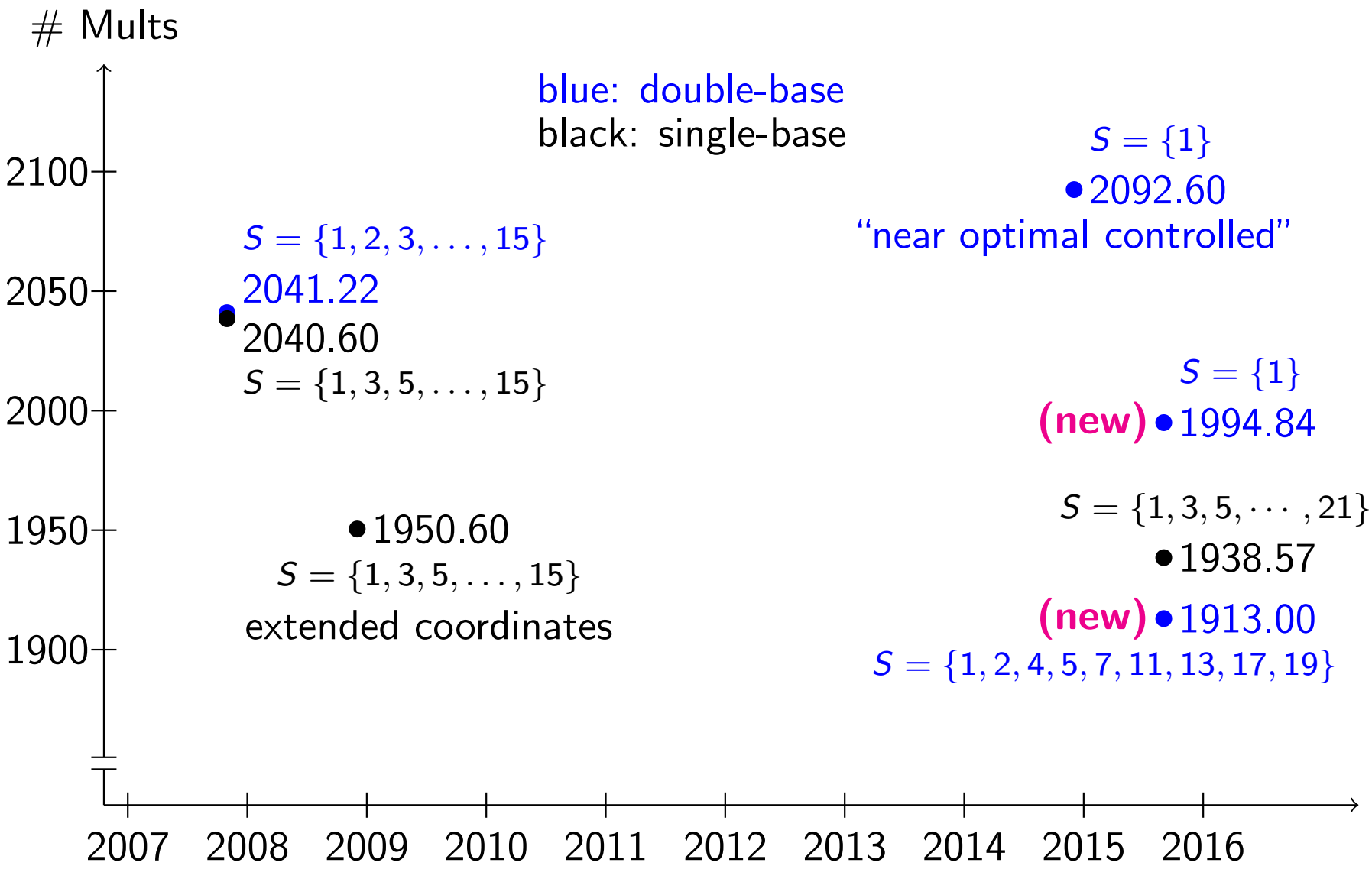
Single- VS Double-base

Scalar multiplication for 256-bit integer on Edwards curve



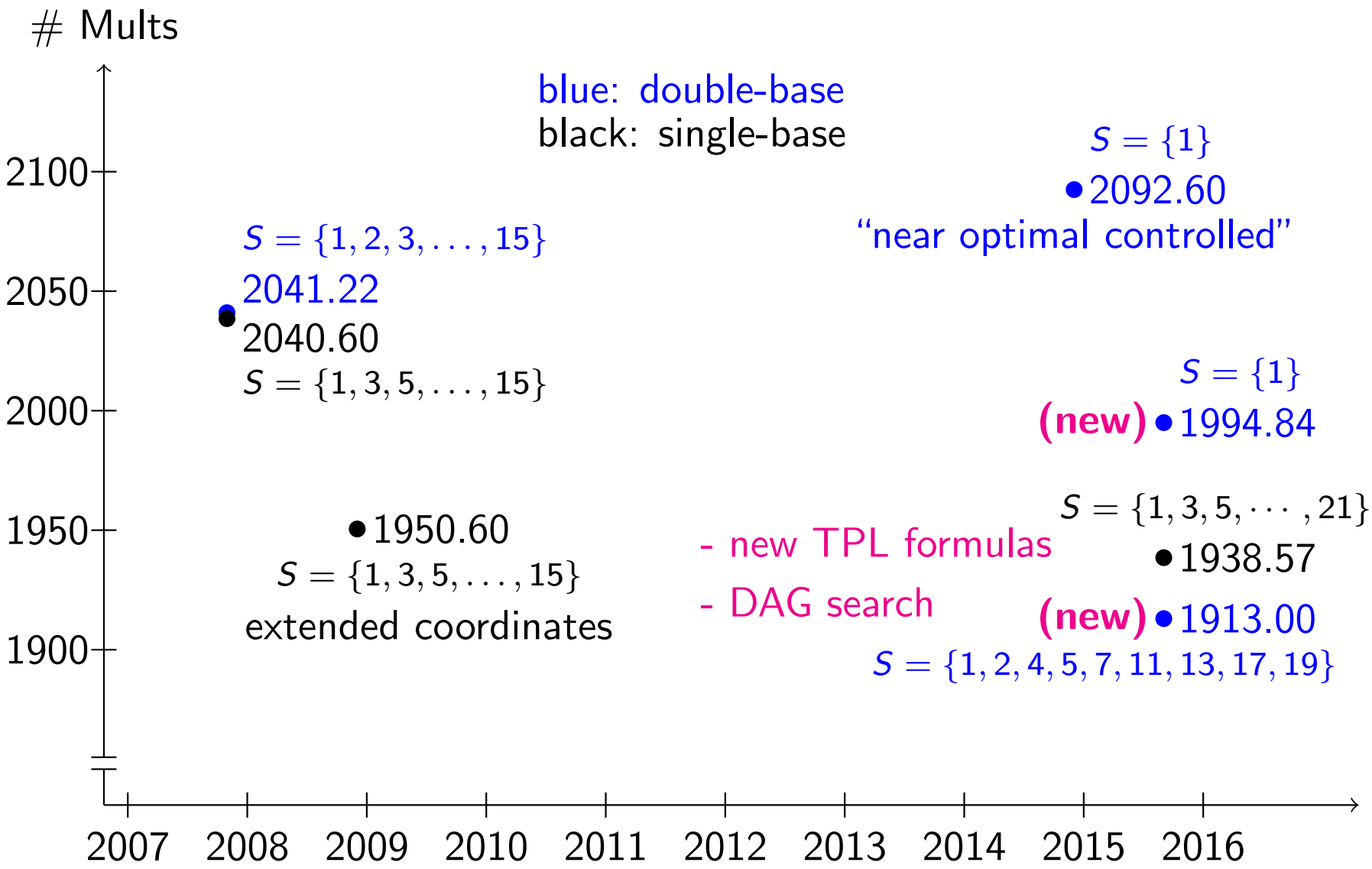
Single- VS Double-base

Scalar multiplication for 256-bit integer on Edwards curve



Single- VS Double-base

Scalar multiplication for 256-bit integer on Edwards curve



Methods

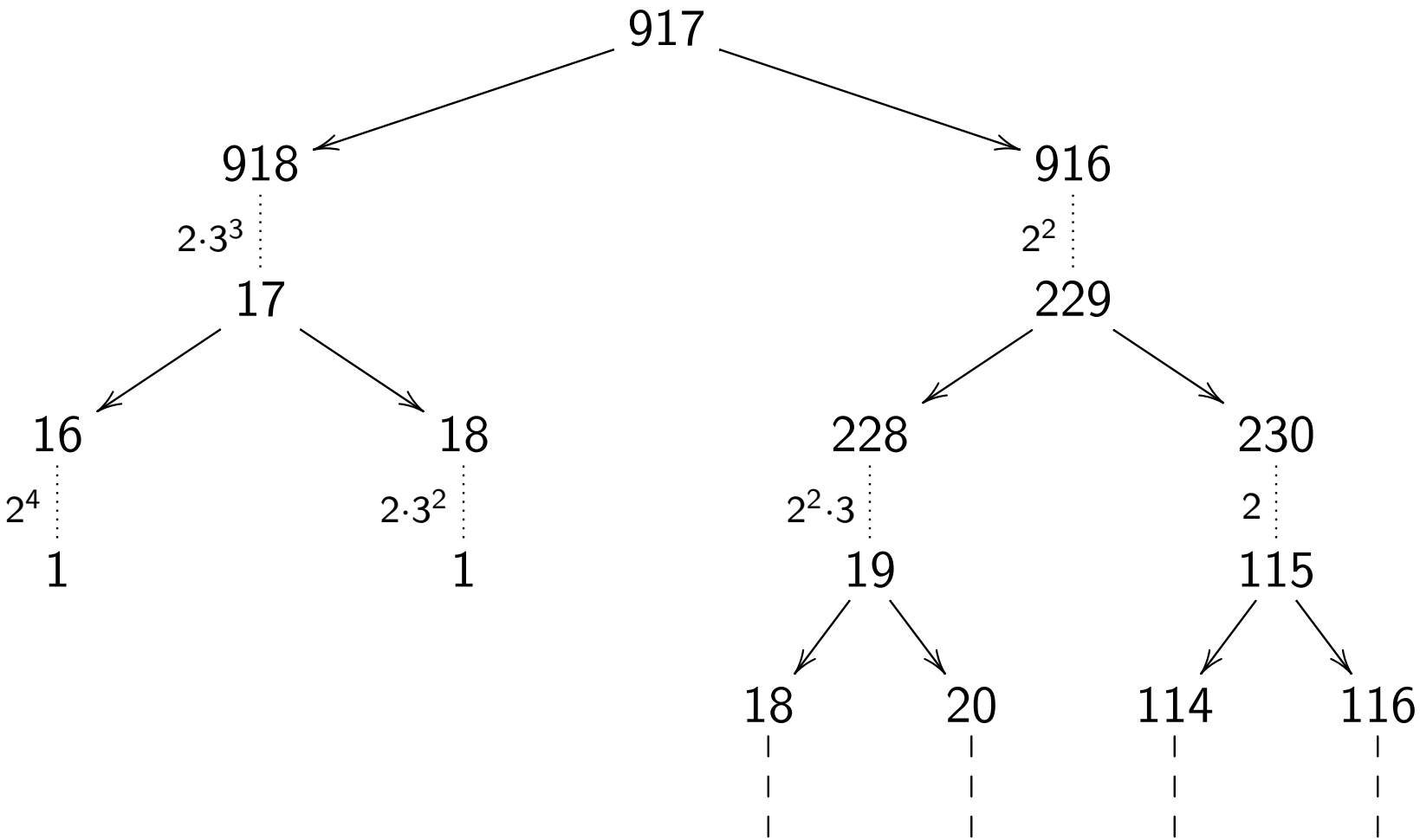
- Faster point tripling formulas
  - twisted Edwards curve
  - one field squaring removed
  - $9\mathbf{M} + 4\mathbf{S} \quad \rightarrow \quad 9\mathbf{M} + 3\mathbf{S}$
  - see https://hyperelliptic.org/EFD/

Methods

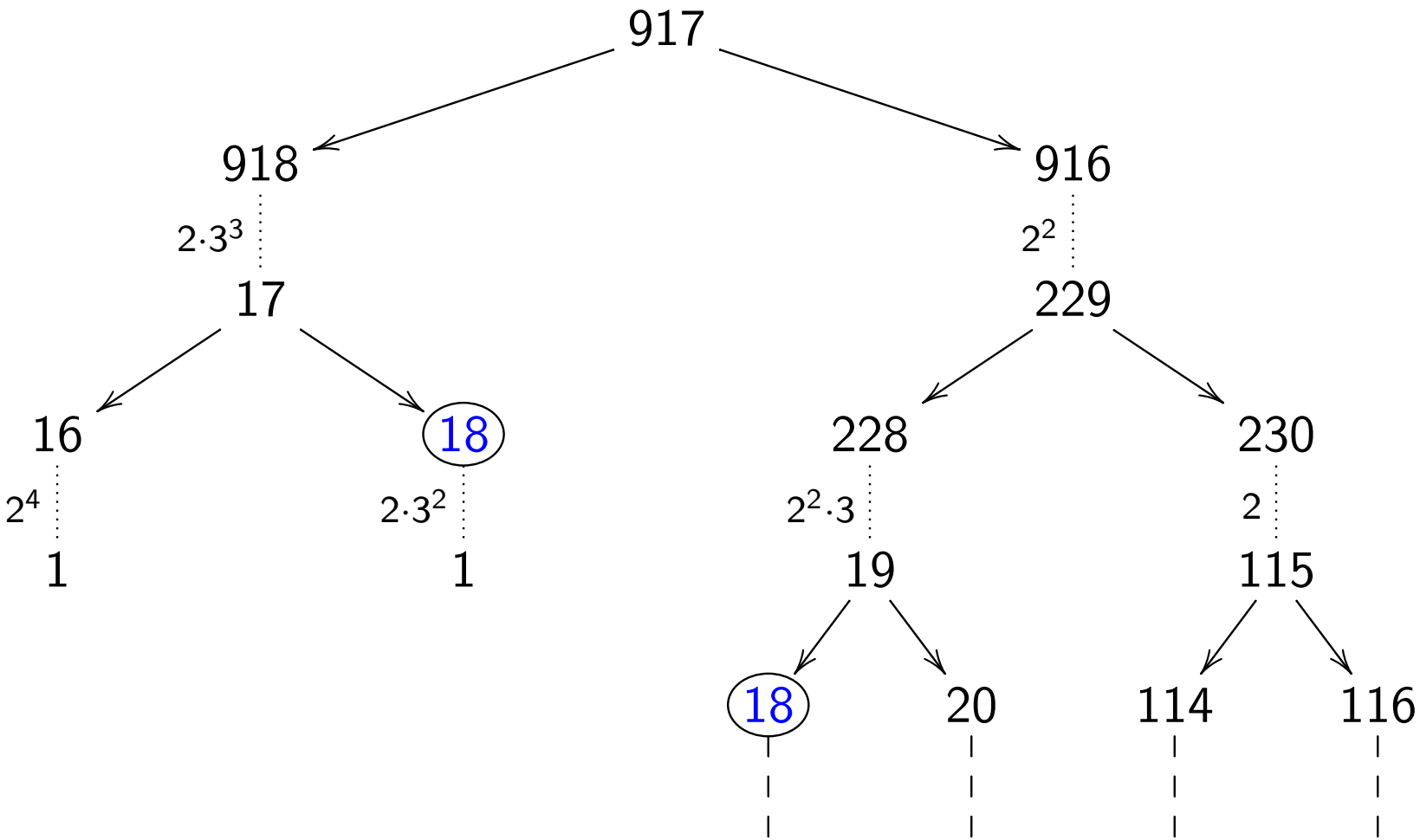
- Faster point tripling formulas
  - twisted Edwards curve
  - one field squaring removed
  - $9\mathbf{M} + 4\mathbf{S} \quad \rightarrow \quad 9\mathbf{M} + 3\mathbf{S}$
  - see https://hyperelliptic.org/EFD/

- Different approach to generate double-base chain
  - use directed acyclic graph instead of tree
  - work with residue class
  - consider addition even if divisible by 2 and/or 3

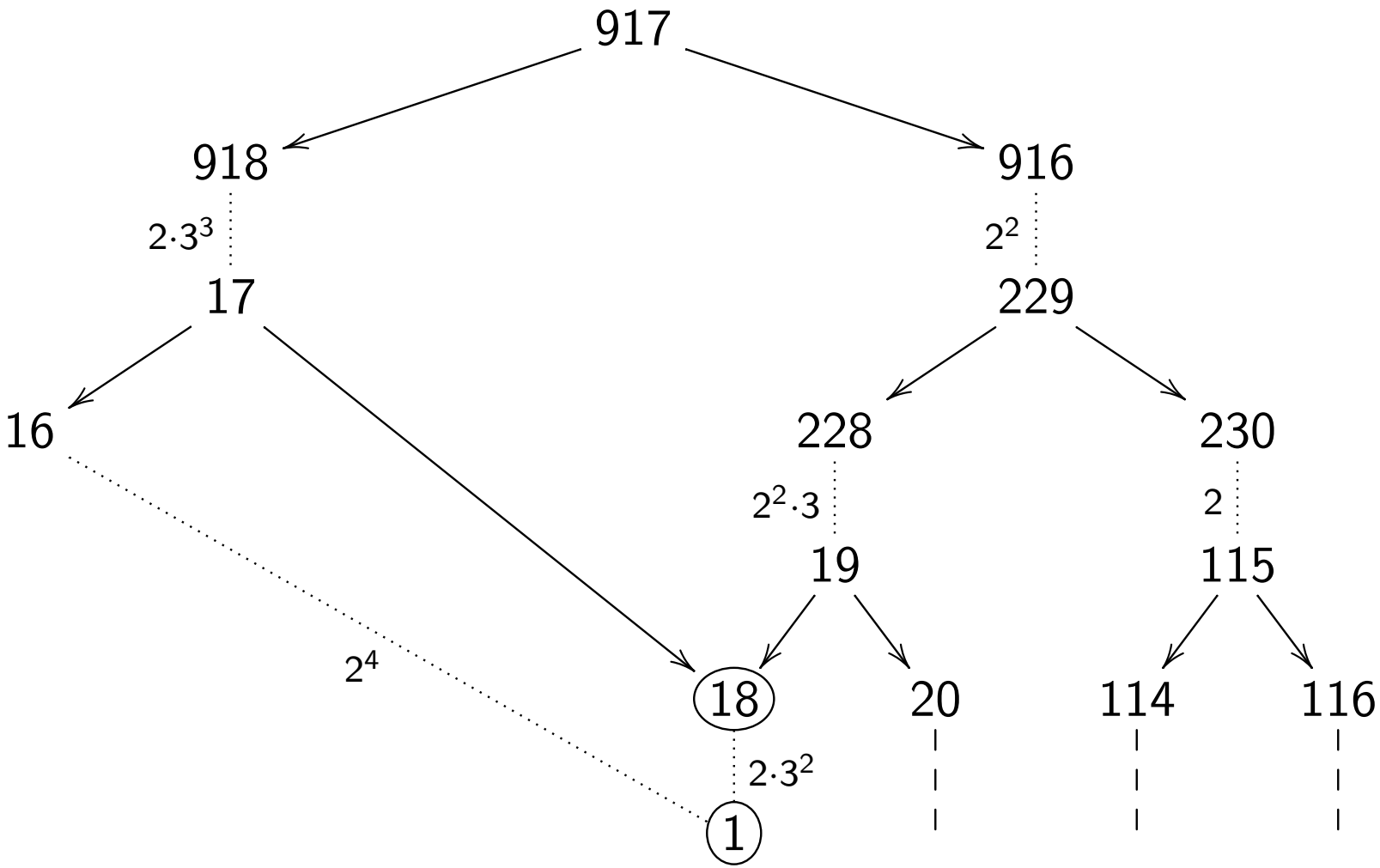
Tree search


917
918
916
$2 \cdot 3^3$
2^2
17
229
16
18
228
230
2^4
$2 \cdot 3^2$
$2^2 \cdot 3$
2
1
1
19
115
18
20
114
116

Tree search


917
918
916
$2 \cdot 3^3$
2^2
17
229
16
18
228
230
2^4
$2 \cdot 3^2$
$2^2 \cdot 3$
2
1
1
19
115
18
20
114
116

Directed-acyclic-graph search



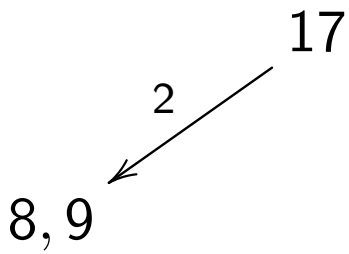
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)

$$17$$

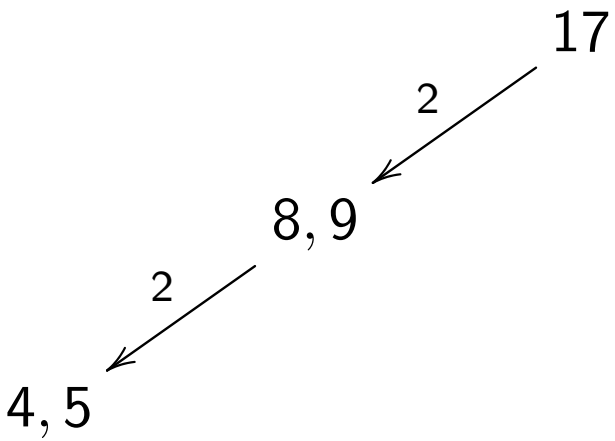
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)



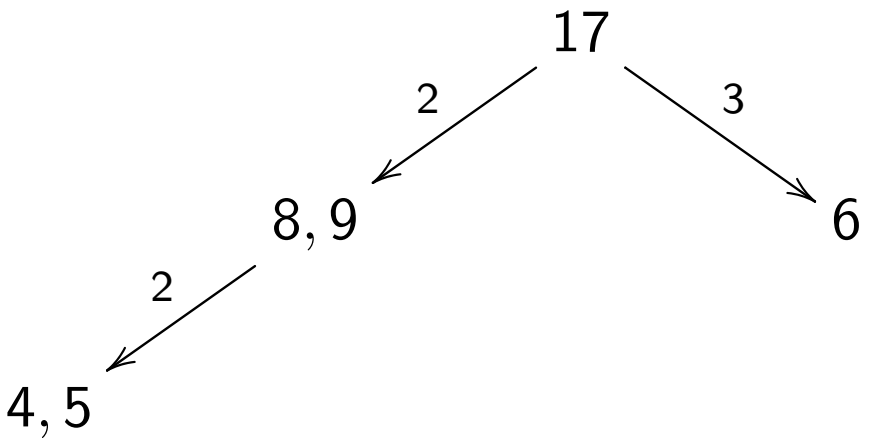
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)



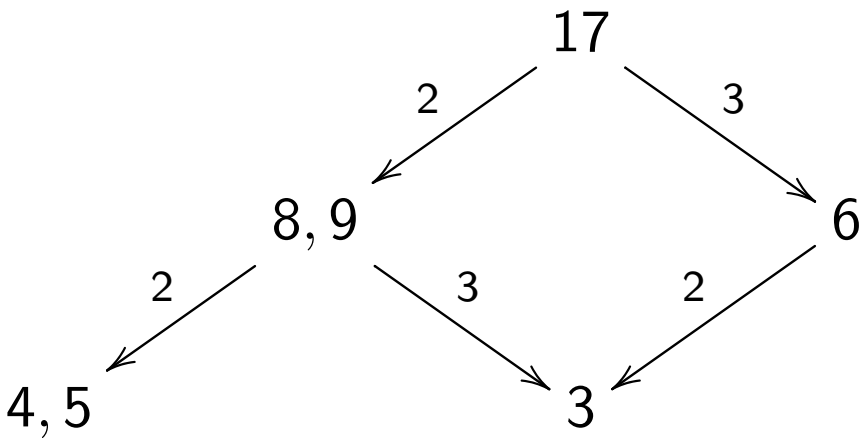
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)



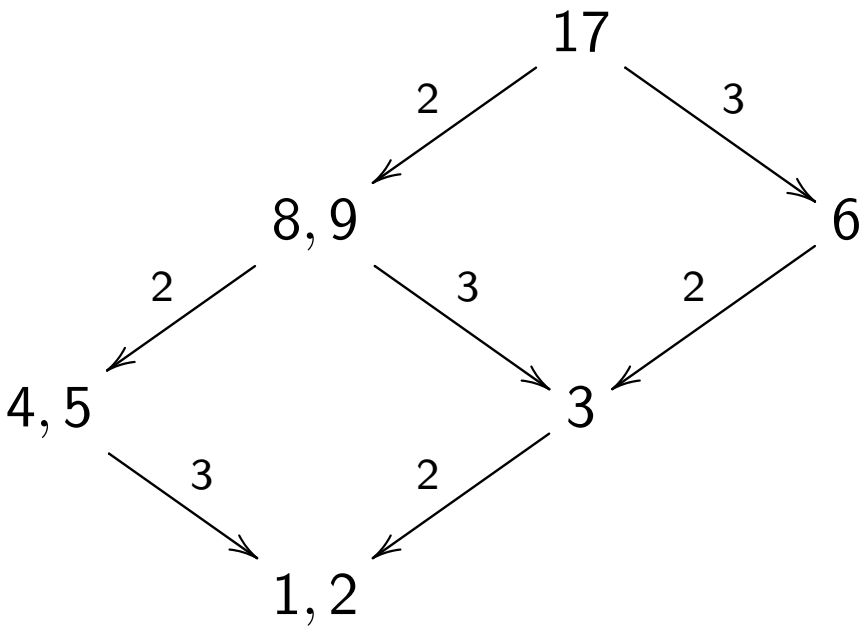
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)



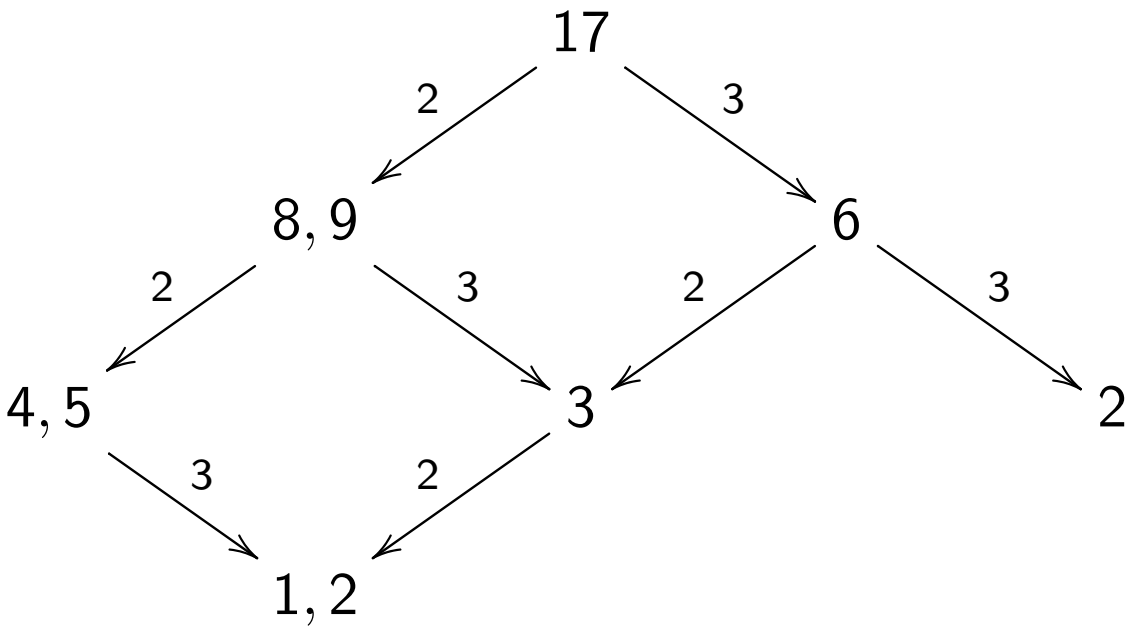
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)



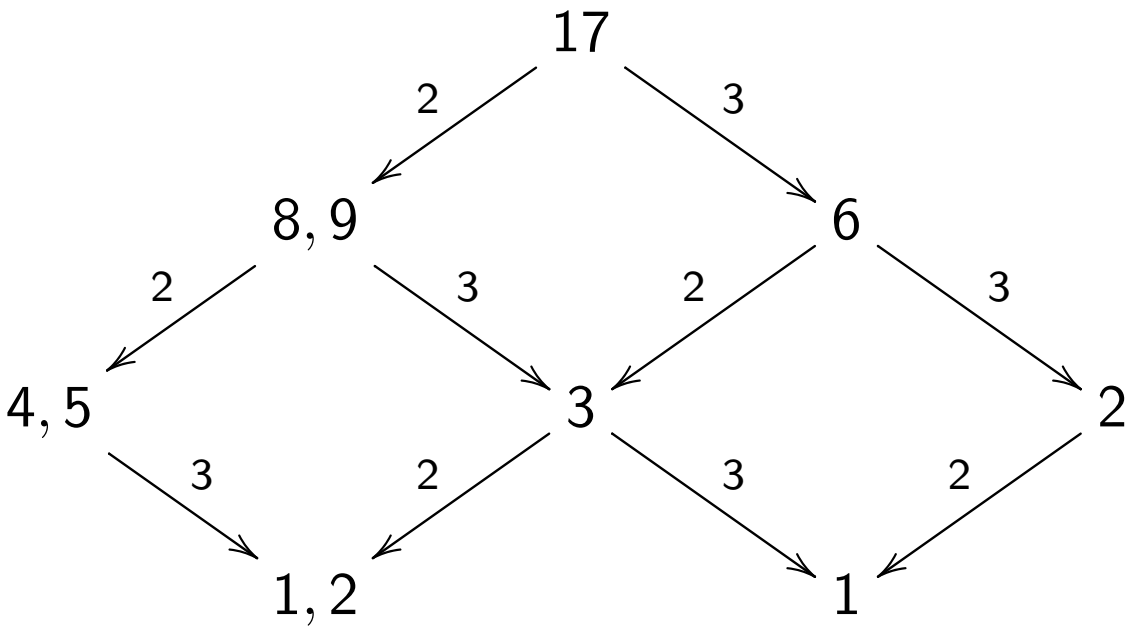
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)



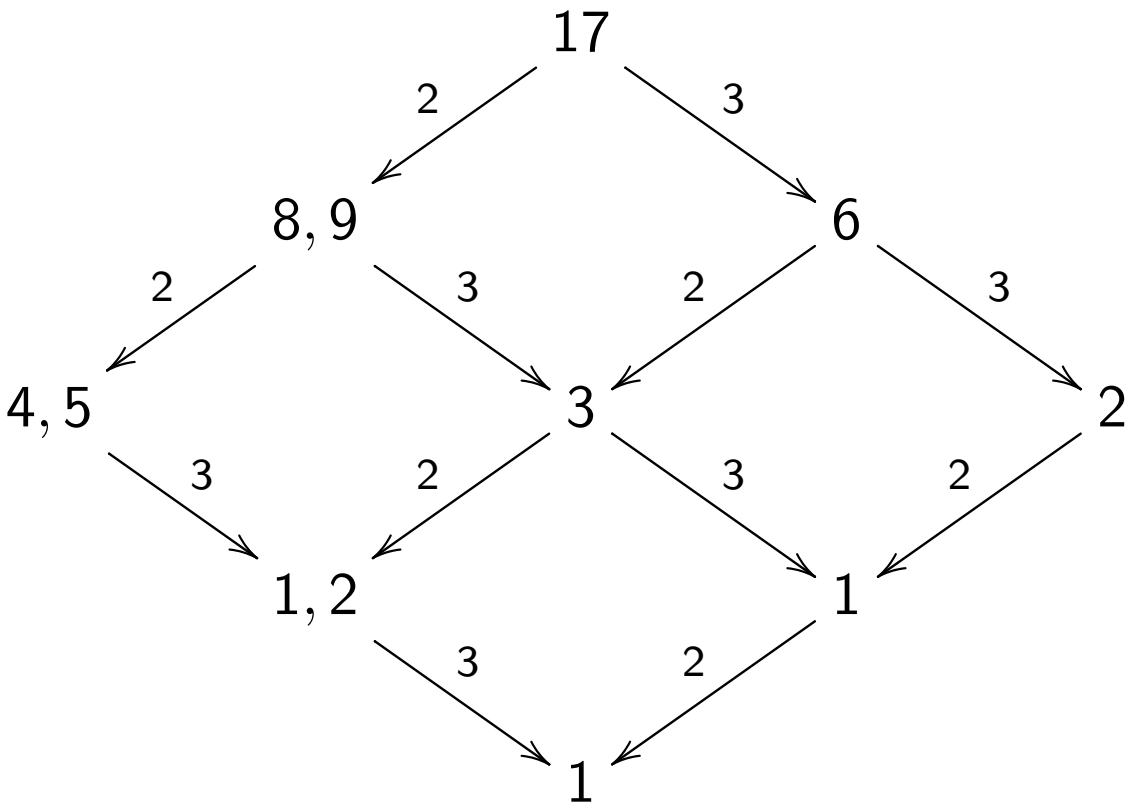
Residue class

- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)

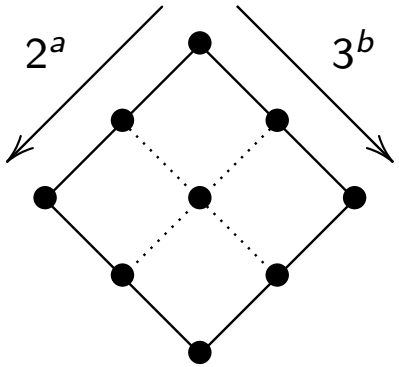


Residue class

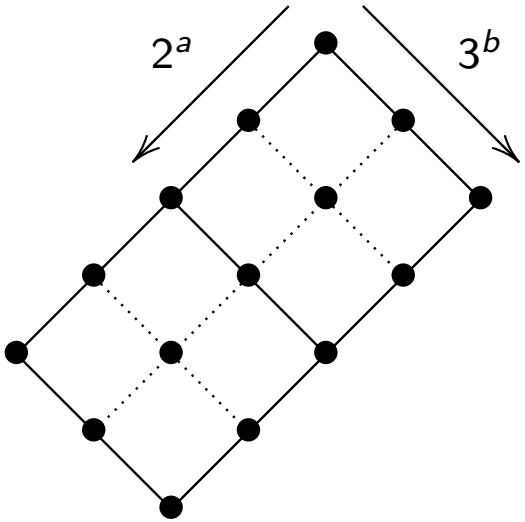
- faster computation of the chain working with smaller number
- e.g. $917 = 17 \bmod 2^2 \cdot 3^2$ (10 bits $\rightarrow$ 5 bits)



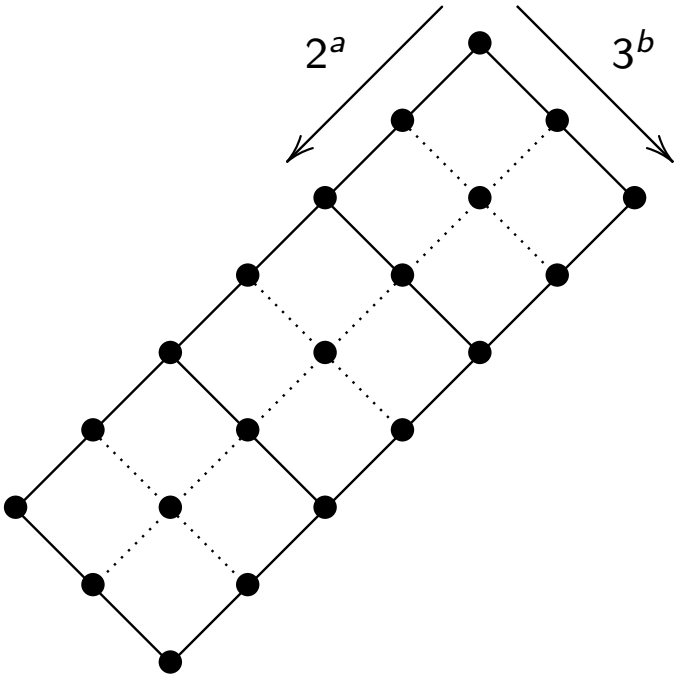
Residue class



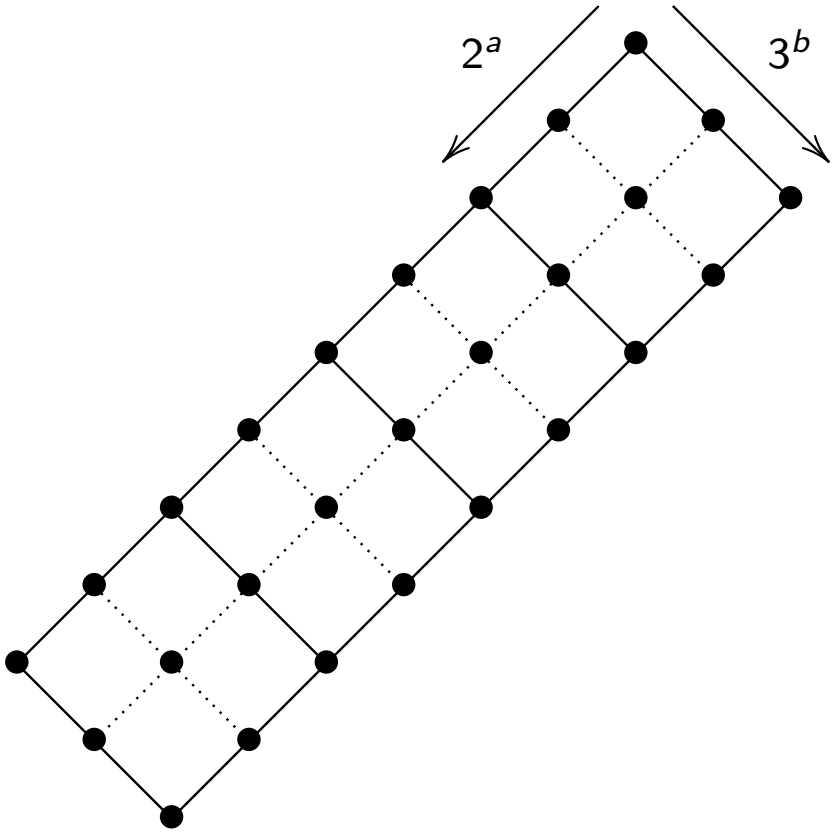
Residue class



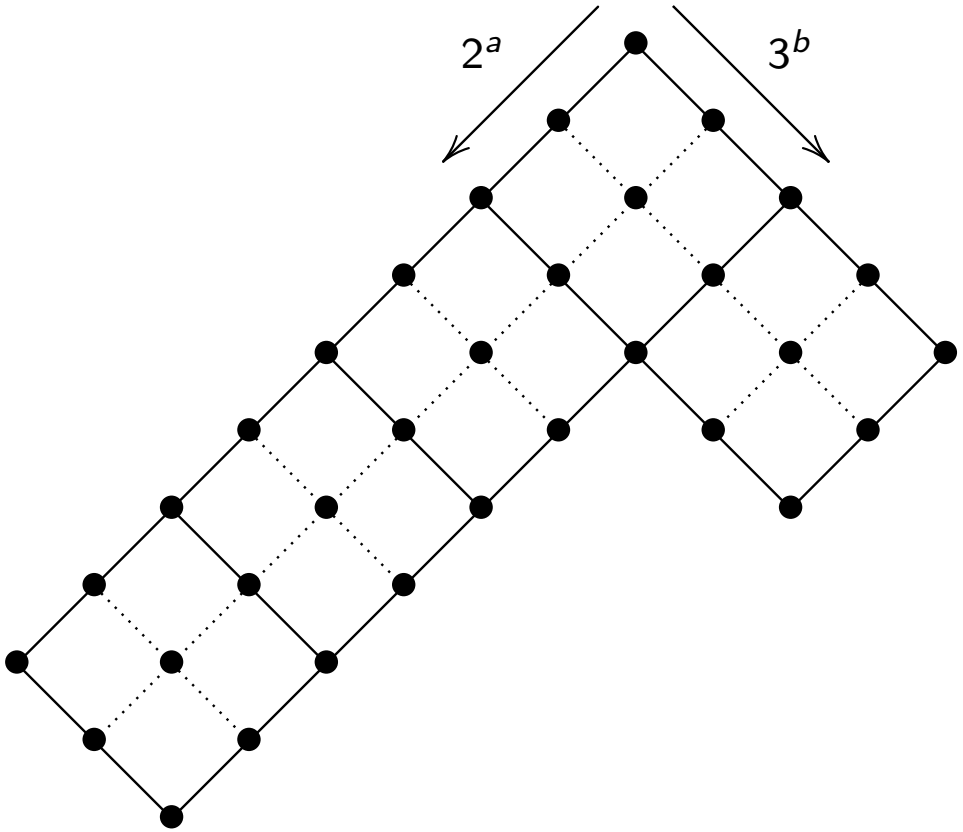
Residue class



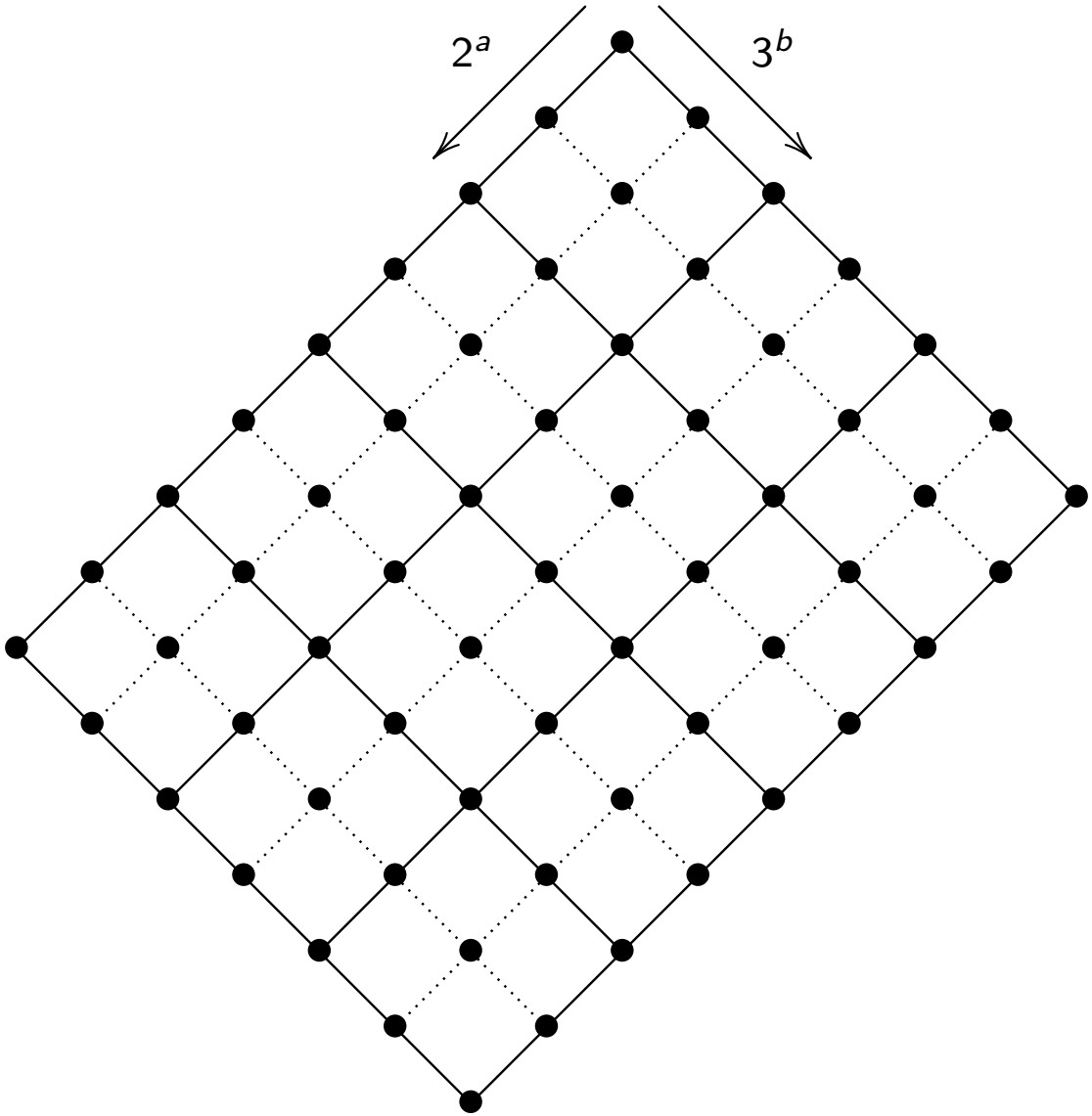
Residue class



Residue class



Residue class



Comparison

	Mults	Mults/ℓ	Precompute set		
single-base	2170.39	8.47808	$\{1\}$	new	
	1947.55	7.60762	$\{1,3,5,7,\ldots,31\}$	new	
	1939.85	7.57752	$\{1,3,5,7,\ldots,17\}$	new	
	1939.02	7.57428	$\{1,3,5,7,\ldots,25\}$	new	
	1938.57	7.57252	$\{1,3,5,7,\ldots,21\}$	new	**(best)**
double-base	2092.60	8.17422	$\{1\}$	AsiaCrypt'14	
	1994.84	7.79233	$\{1\}$	new	
	1915.88	7.48391	$\{1,2,4,5,7,11,13\}$	new	
	1914.91	7.48010	$\{1,5,7,11,13,17,19,23,25\}$	new	
	1913.14	7.47320	$\{1,5,7,11,13,17,19\}$	new	
	1913.00	7.47266	$\{1,2,4,5,7,11,13,17,19\}$	new	**(best)**