Curve25519: Implementations and Applications

Tung Chou

Technische Universiteit Eindhoven, The Netherlands

Part 1:

Sandy2x: new Curve25519 speed records

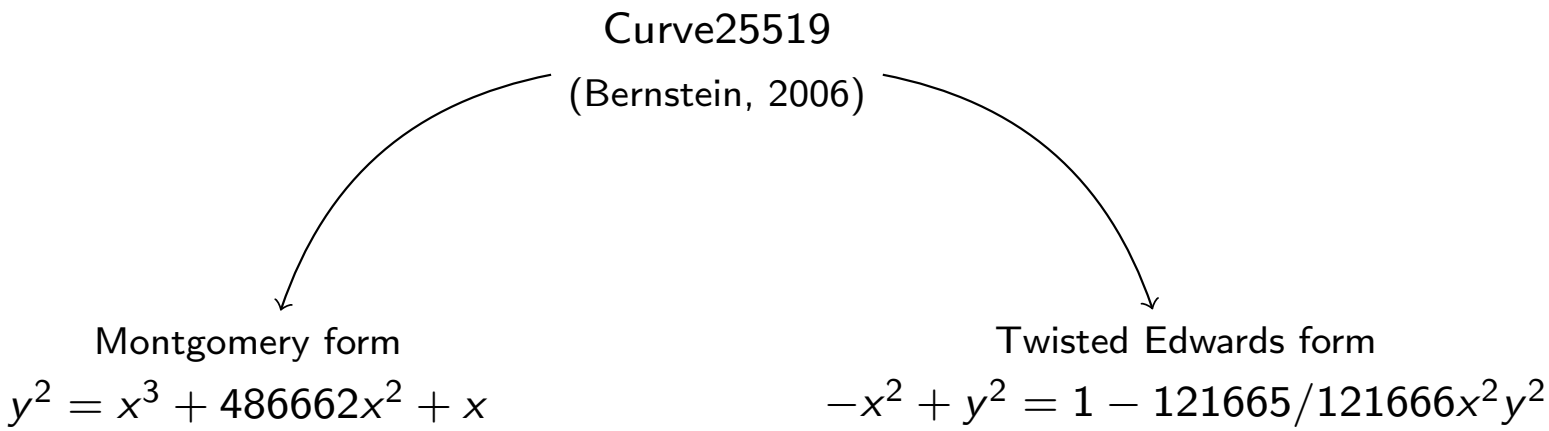
Part 2:

The simplest protocol for oblivious transfer

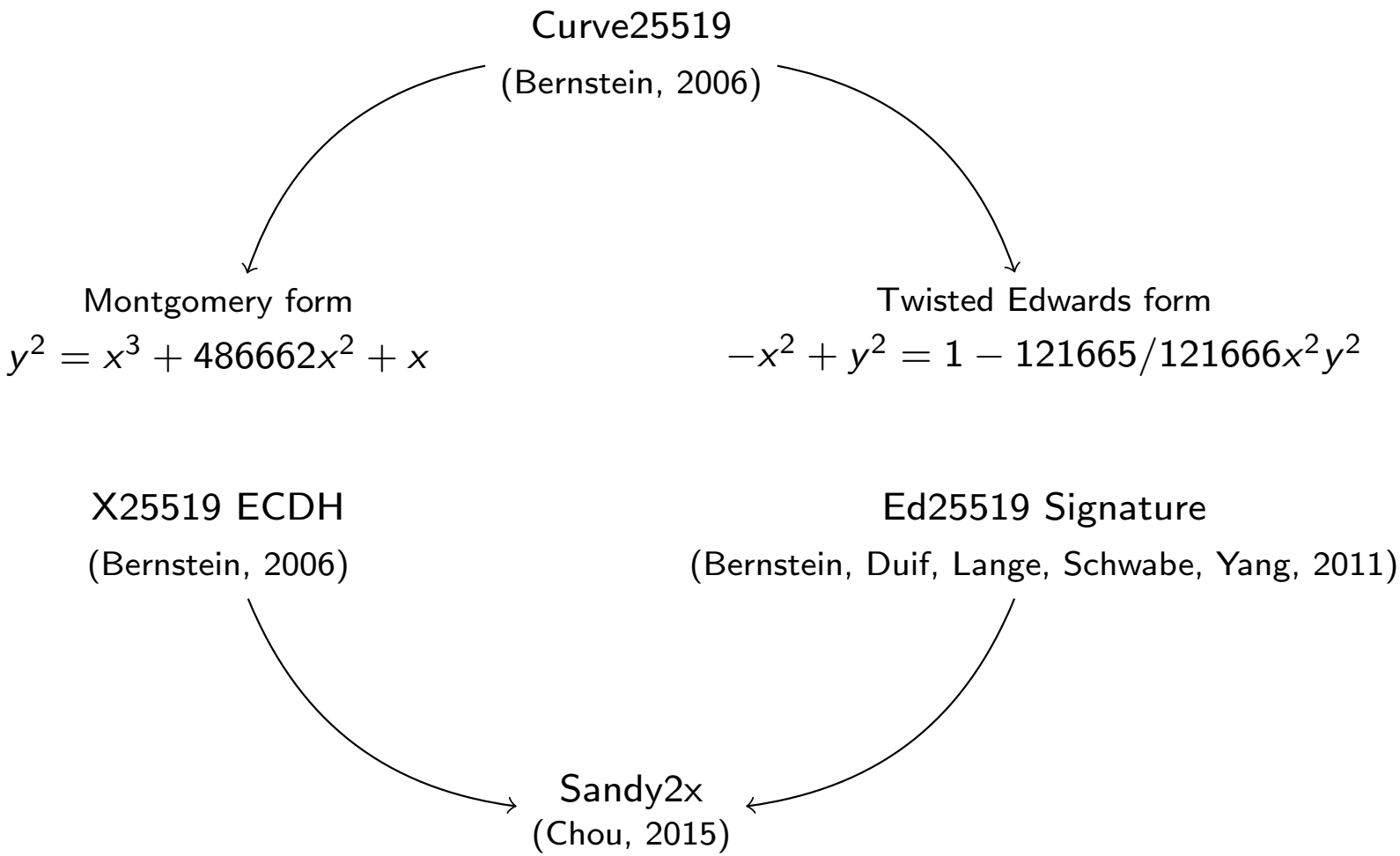
(Joint work with Claudio Orlandi)

Part 1.

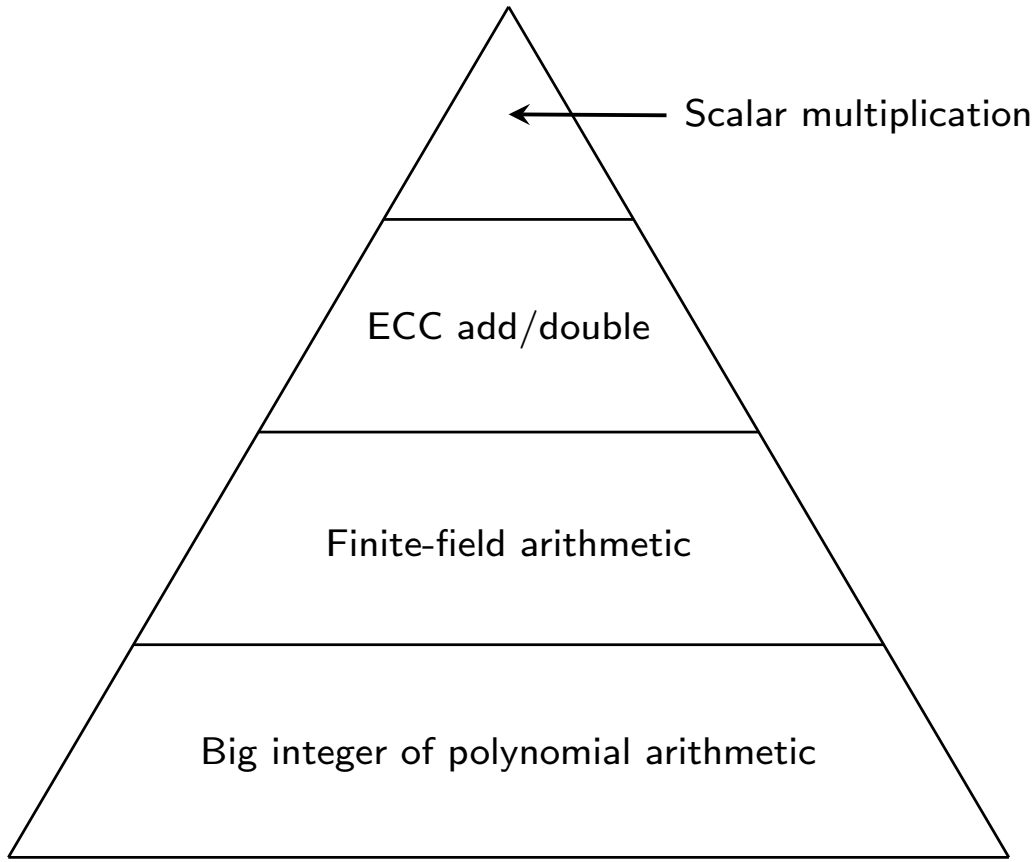
Sandy2x


Curve25519
(Bernstein, 2006)
Montgomery form
$y^2 = x^3 + 486662x^2 + x$
Twisted Edwards form
$-x^2 + y^2 = 1 - 121665/121666x^2y^2$

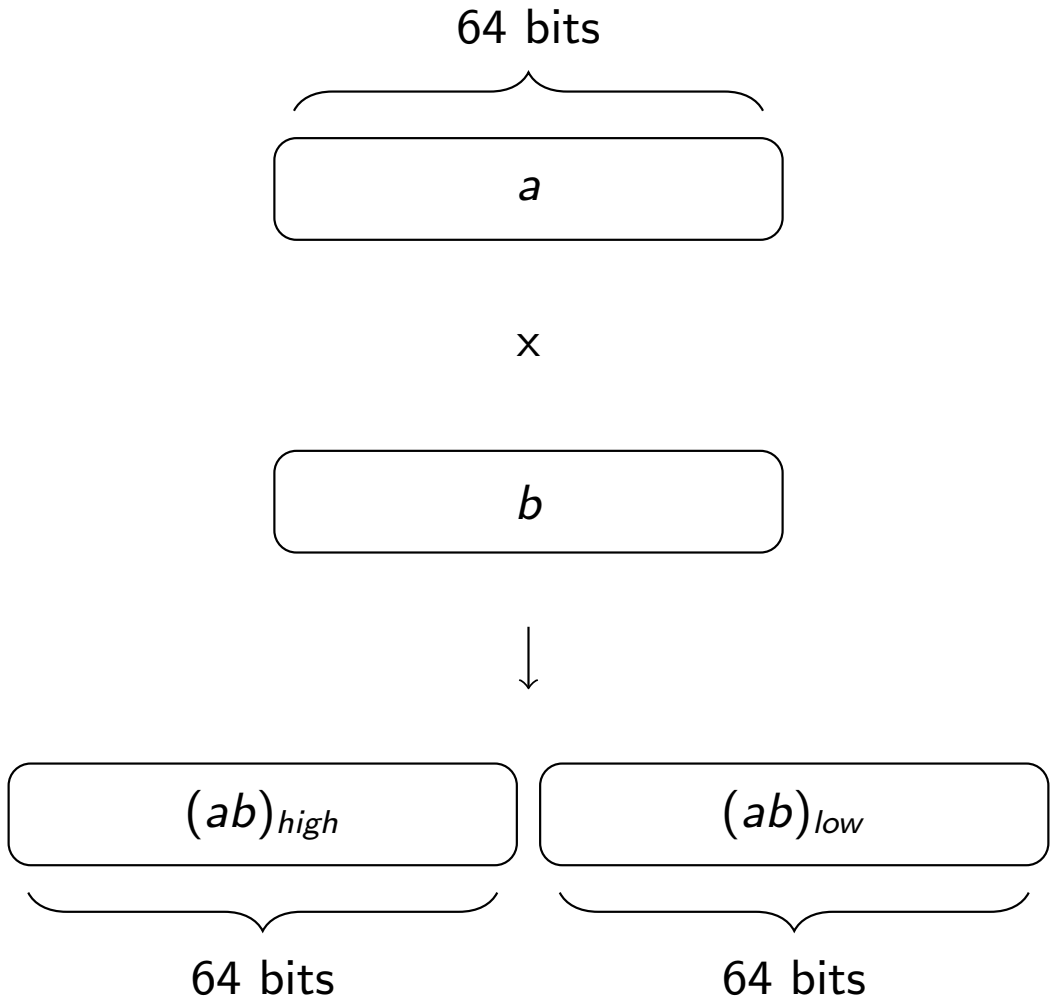
Sandy2x


Curve25519
(Bernstein, 2006)
Montgomery form
$y^2 = x^3 + 486662x^2 + x$
Twisted Edwards form
$-x^2 + y^2 = 1 - 121665/121666x^2y^2$
X25519 ECDH
(Bernstein, 2006)
Ed25519 Signature
(Bernstein, Duif, Lange, Schwabe, Yang, 2011)
Sandy2x
(Chou, 2015)

The ECC implementation pyramid



The big multiplier



The radix-2^{51} representation for $\mathbb{F}_{2^{255}-19}$

The radix-2^{51} representation for $\mathbb{F}_{2^{255}-19}$

$$f = f_0 + f_1 2^{51} + f_2 2^{102} + f_3 2^{153} + f_4 2^{204}$$

The radix-2^{51} representation for $\mathbb{F}_{2^{255}-19}$

$$\begin{array}{rccccc} f = & f_0 + & f_1 2^{51} + & f_2 2^{102} + & f_3 2^{153} + & f_4 2^{204} \\ g = & g_0 + & g_1 2^{51} + & g_2 2^{102} + & g_3 2^{153} + & g_4 2^{204} \end{array}$$

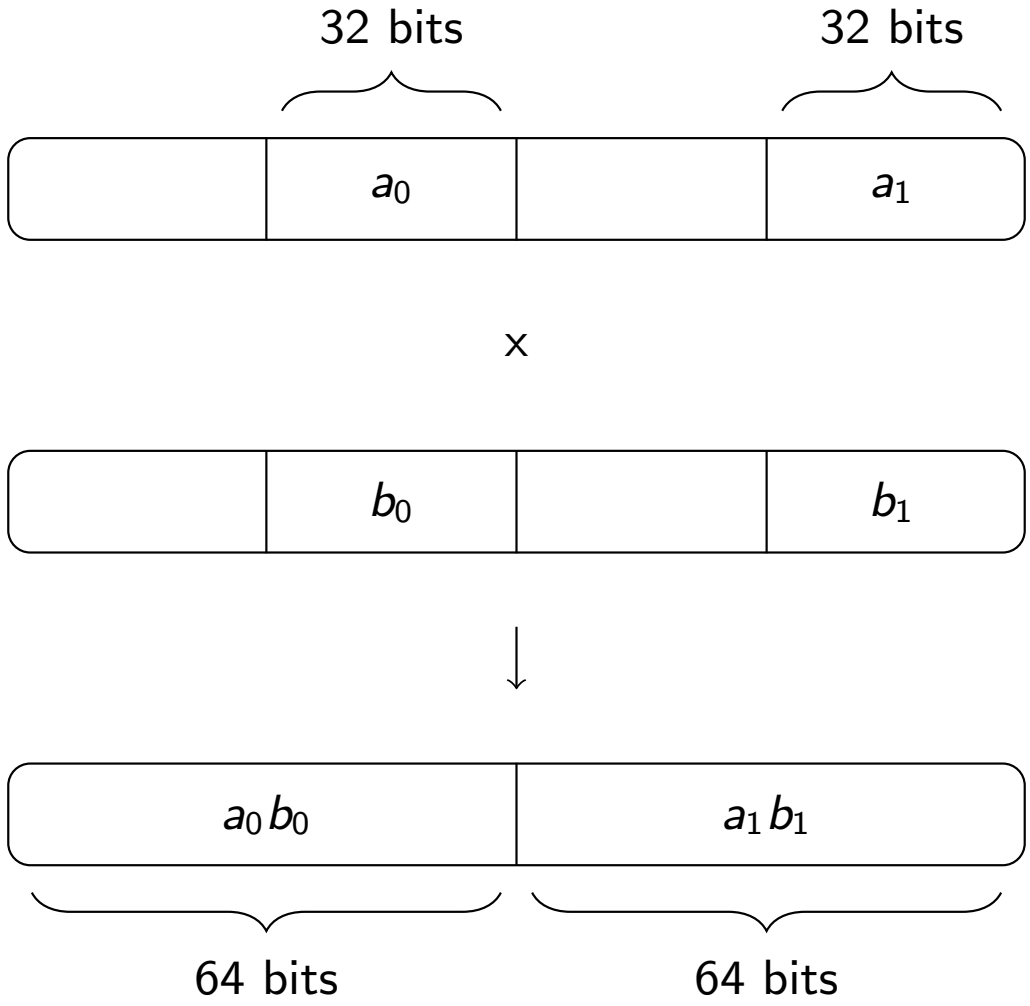
The radix-2^{51} representation for $\mathbb{F}_{2^{255}-19}$

$$
\begin{aligned}
f = {} & f_0 + & f_1 2^{51} + & & f_2 2^{102} + & & f_3 2^{153} + & & f_4 2^{204} \\
g = {} & g_0 + & g_1 2^{51} + & & g_2 2^{102} + & & g_3 2^{153} + & & g_4 2^{204}
\end{aligned}
$$

$$
\Big\downarrow \times \pmod{2^{255}-19}
$$

$$
\begin{aligned}
h_0 = {} & f_0 g_0 + & 19 f_1 g_4 + & & 19 f_2 g_3 + & & 19 f_3 g_2 + & & 19 f_4 g_1 \\
h_1 = {} & f_0 g_1 + & f_1 g_0 + & & 19 f_2 g_4 + & & 19 f_3 g_3 + & & 19 f_4 g_2 \\
h_2 = {} & f_0 g_2 + & f_1 g_1 + & & f_2 g_0 + & & 19 f_3 g_4 + & & 19 f_4 g_3 \\
h_3 = {} & f_0 g_3 + & f_1 g_2 + & & f_2 g_1 + & & f_3 g_0 + & & 19 f_4 g_4 \\
h_4 = {} & f_0 g_4 + & f_1 g_3 + & & f_2 g_2 + & & f_3 g_1 + & & f_4 g_0
\end{aligned}
$$

A small multiplier



The radix-$2^{25.5}$ representation for $\mathbb{F}_{2^{255}-19}$

$$
\begin{aligned}
f &= f_0 + f_1 2^{26} + f_2 2^{51} + f_3 2^{77} + f_4 2^{102} + f_5 2^{128} + f_6 2^{153} + f_7 2^{179} + f_8 2^{204} + f_9 2^{230} \\
g &= g_0 + g_1 2^{26} + g_2 2^{51} + g_3 2^{77} + g_4 2^{102} + g_5 2^{128} + g_6 2^{153} + g_7 2^{179} + g_8 2^{204} + g_9 2^{230}
\end{aligned}
$$

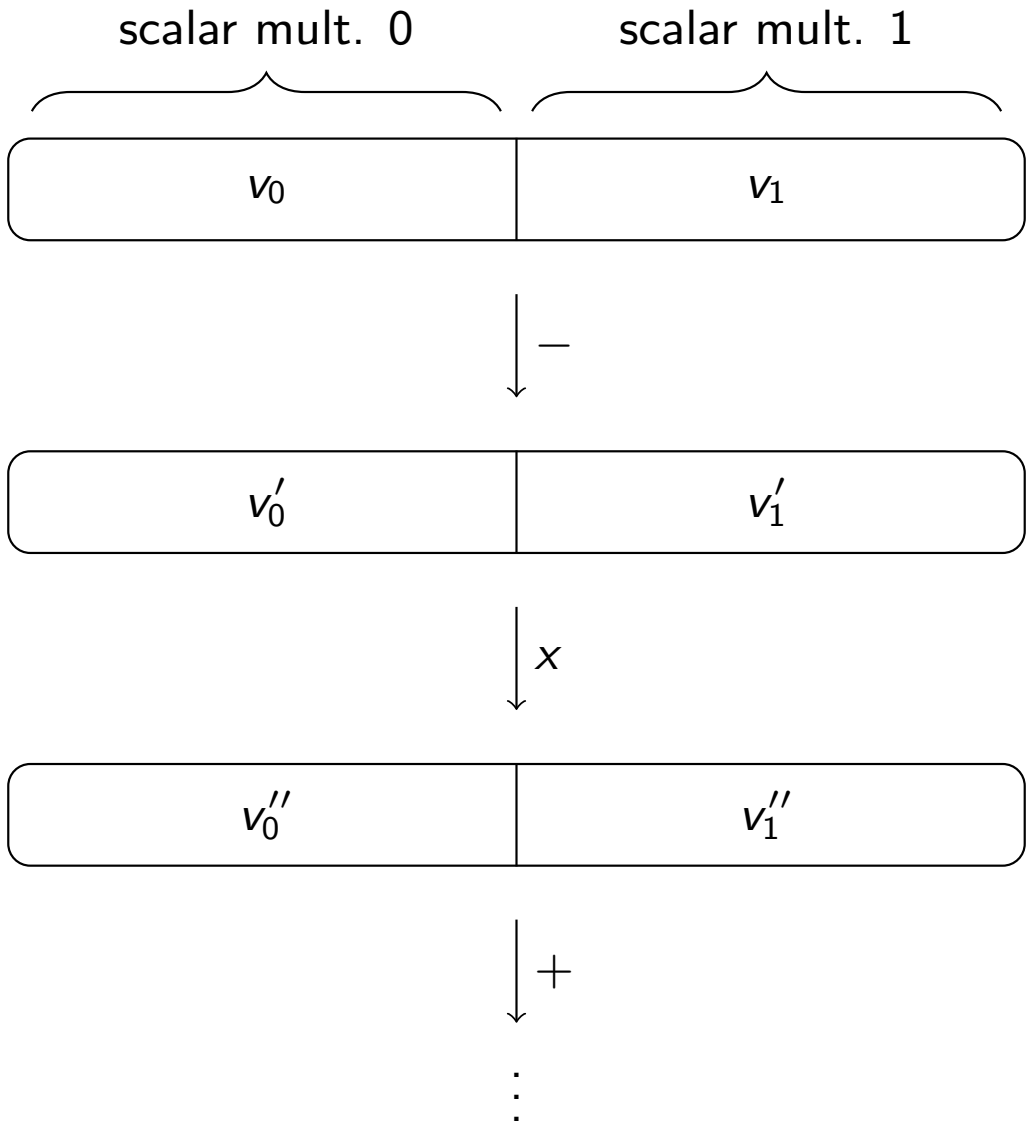
The radix-$2^{25.5}$ representation for $\mathbb{F}_{2^{255}-19}$

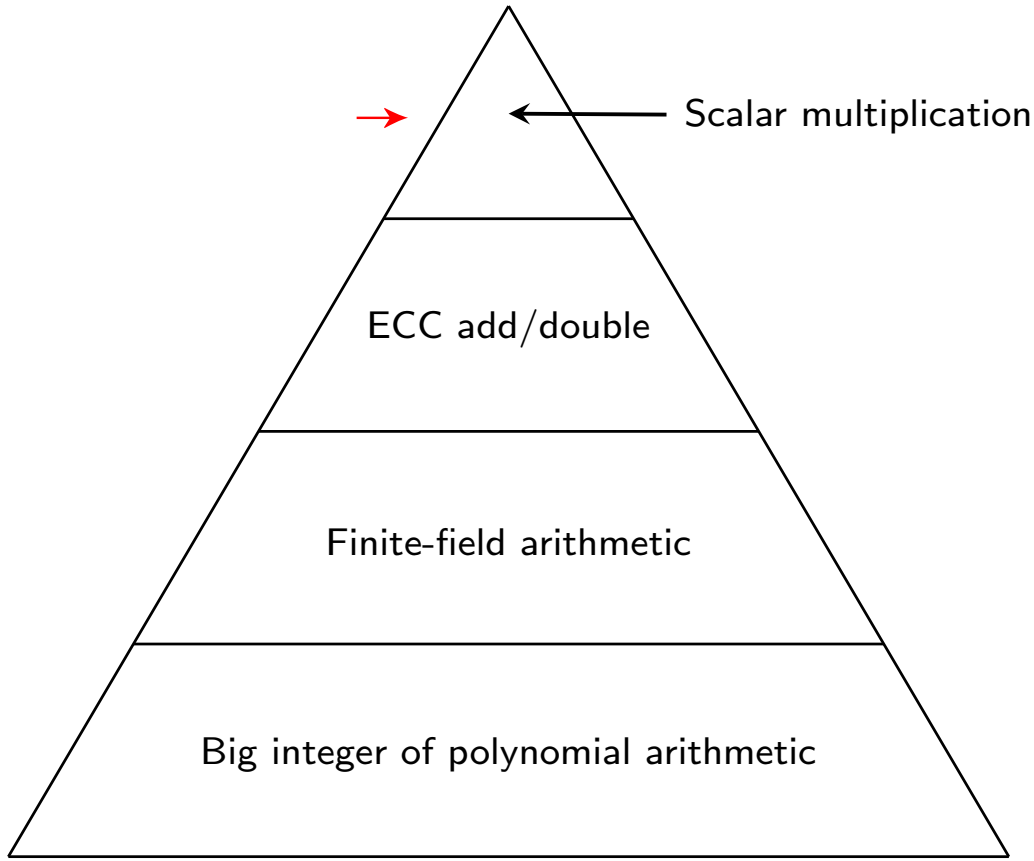
$$
\begin{aligned}
f &= f_0 + f_1 2^{26} + f_2 2^{51} + f_3 2^{77} + f_4 2^{102} + f_5 2^{128} + f_6 2^{153} + f_7 2^{179} + f_8 2^{204} + f_9 2^{230} \\
g &= g_0 + g_1 2^{26} + g_2 2^{51} + g_3 2^{77} + g_4 2^{102} + g_5 2^{128} + g_6 2^{153} + g_7 2^{179} + g_8 2^{204} + g_9 2^{230}
\end{aligned}
$$

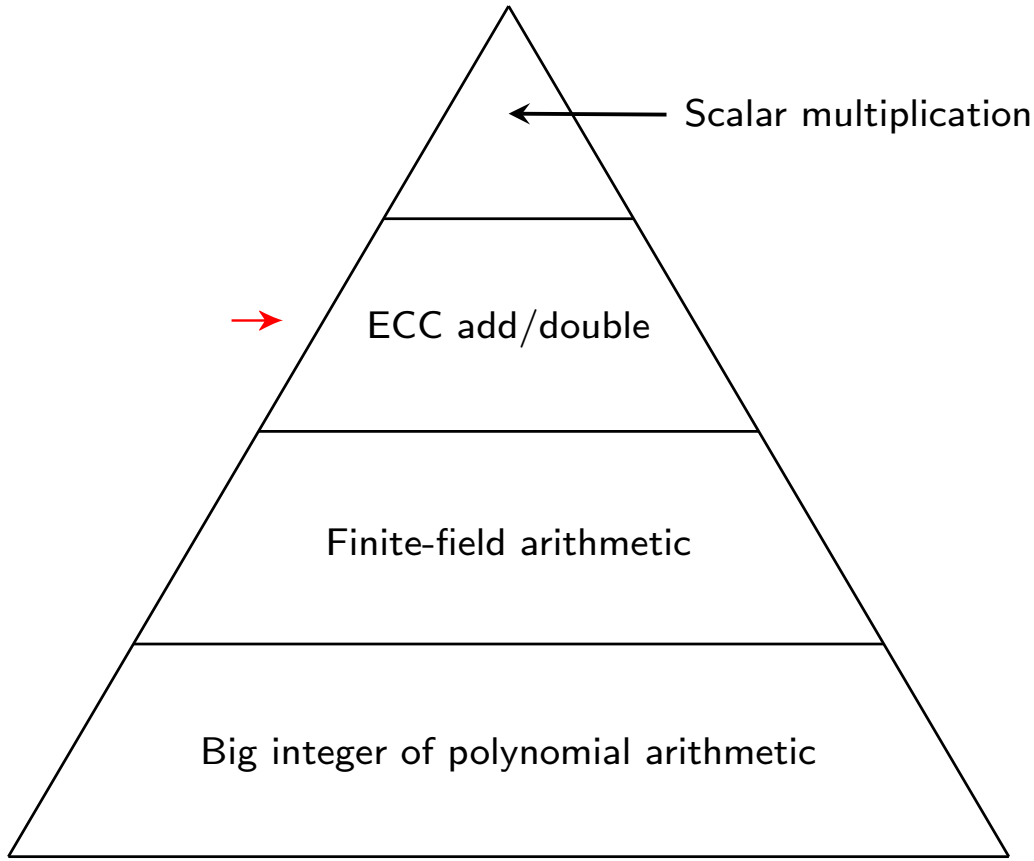
$$
\downarrow \times \pmod{2^{255}-19}
$$

$$
\begin{aligned}
h_0 &= f_0g_0 + 38f_1g_9 + 19f_2g_8 + 38f_3g_7 + 19f_4g_6 + 38f_5g_5 + 19f_6g_4 + 38f_7g_3 + 19f_8g_2 + 38f_9g_1 \\
h_1 &= f_0g_1 + f_1g_0 + 19f_2g_9 + 19f_3g_8 + 19f_4g_7 + 19f_5g_6 + 19f_6g_5 + 19f_7g_4 + 19f_8g_3 + 19f_9g_2 \\
h_2 &= f_0g_2 + 2f_1g_1 + f_2g_0 + 38f_3g_9 + 19f_4g_8 + 38f_5g_7 + 19f_6g_6 + 38f_7g_5 + 19f_8g_4 + 38f_9g_3 \\
h_3 &= f_0g_3 + f_1g_2 + f_2g_1 + f_3g_0 + 19f_4g_9 + 19f_5g_8 + 19f_6g_7 + 19f_7g_6 + 19f_8g_5 + 19f_9g_4 \\
h_4 &= f_0g_4 + 2f_1g_3 + f_2g_2 + 2f_3g_1 + f_4g_0 + 38f_5g_9 + 19f_6g_8 + 38f_7g_7 + 19f_8g_6 + 38f_9g_5 \\
h_5 &= f_0g_5 + f_1g_4 + f_2g_3 + f_3g_2 + f_4g_1 + f_5g_0 + 19f_6g_9 + 19f_7g_8 + 19f_8g_7 + 19f_9g_6 \\
h_6 &= f_0g_6 + 2f_1g_5 + f_2g_4 + 2f_3g_3 + f_4g_2 + 2f_5g_1 + f_6g_0 + 38f_7g_9 + 19f_8g_8 + 38f_9g_7 \\
h_7 &= f_0g_7 + f_1g_6 + f_2g_5 + f_3g_4 + f_4g_3 + f_5g_2 + f_6g_1 + f_7g_0 + 19f_8g_9 + 19f_9g_8 \\
h_8 &= f_0g_8 + 2f_1g_7 + f_2g_6 + 2f_3g_5 + f_4g_4 + 2f_5g_3 + f_6g_2 + 2f_7g_1 + f_8g_0 + 38f_9g_9 \\
h_9 &= f_0g_9 + f_1g_8 + f_2g_7 + f_3g_6 + f_4g_5 + f_5g_4 + f_6g_3 + f_7g_2 + f_8g_1 + f_9g_0
\end{aligned}
$$

External parallelism




Scalar multiplication
ECC add/double
Finite-field arithmetic
Big integer of polynomial arithmetic


Scalar multiplication
ECC add/double
Finite-field arithmetic
Big integer of polynomial arithmetic

Fixed-base scalar multiplication

$$P = sB = s_0 B + s_1 16^1 B + s_2 16^2 B + \cdots + s_{15} 16^{15} B$$

Fixed-base scalar multiplication

$$P = sB = s_0 B + s_1 16^1 B + s_2 16^2 B + \cdots + s_{15} 16^{15} B$$

$$\downarrow$$

$$P_0 = s_0 B + s_2 16^2 B + \cdots + s_{14} 16^{14} B$$

$$P_1 = s_1 B + s_3 16^2 B + \cdots + s_{15} 16^{14} B$$

$$(P = P_0 + 16 P_1)$$

Constant-time table lookup

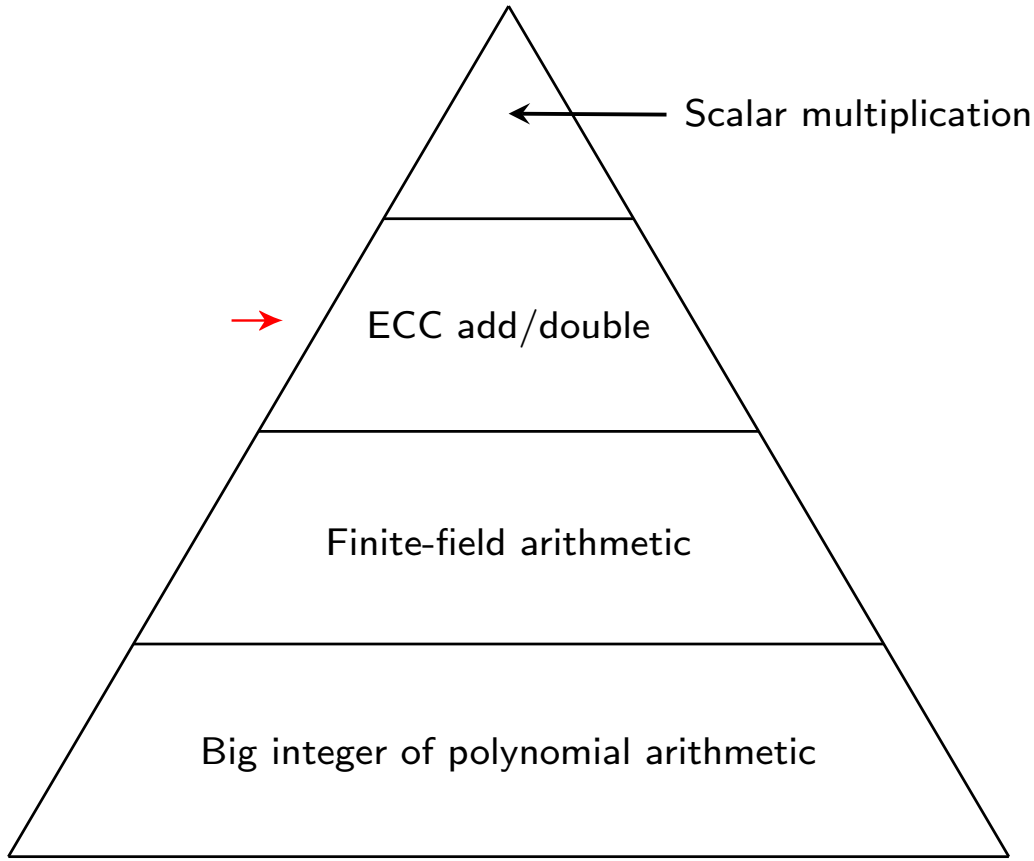
table entries
$0 \cdot 16^k B$
$1 \cdot 16^k B$
⋮
$s_i \cdot 16^k B$
⋮
$15 \cdot 16^k B$

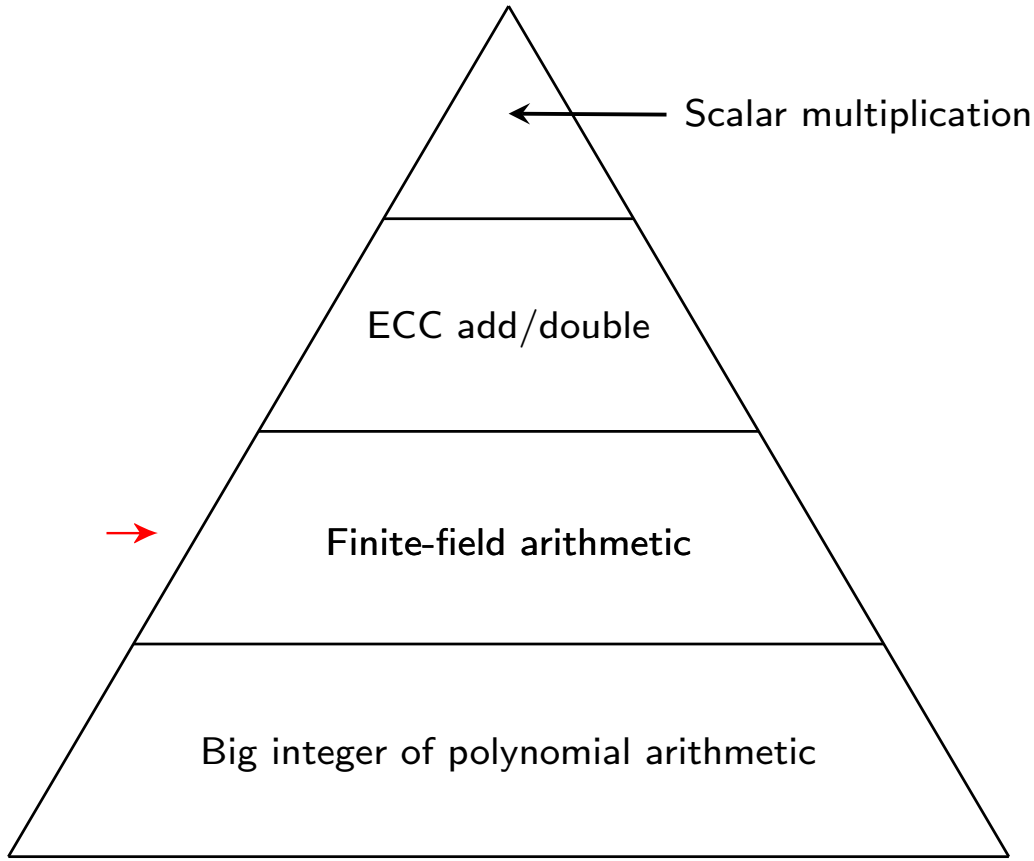
Constant-time table lookup

masks		table entries
$(000\ldots0)_2$	AND	$0 \cdot 16^k B$
$(000\ldots0)_2$	AND	$1 \cdot 16^k B$
$\vdots$		$\vdots$
$(111\ldots1)_2$	AND	$s_i \cdot 16^k B$
$\vdots$		$\vdots$
$(000\ldots0)_2$	AND	$15 \cdot 16^k B$

Constant-time table lookup

masks		table entries
$(000\ldots0)_2$	AND	$0 \cdot 16^k B$
$(000\ldots0)_2$	AND	$1 \cdot 16^k B$
$\vdots$		$\vdots$
$(111\ldots1)_2$	AND	$s_i \cdot 16^k B$
$\vdots$		$\vdots$
$(000\ldots0)_2$	AND	$15 \cdot 16^k B$
$+)$		
		$s_i \cdot 16^k B$


Scalar multiplication
ECC add/double
Finite-field arithmetic
Big integer of polynomial arithmetic

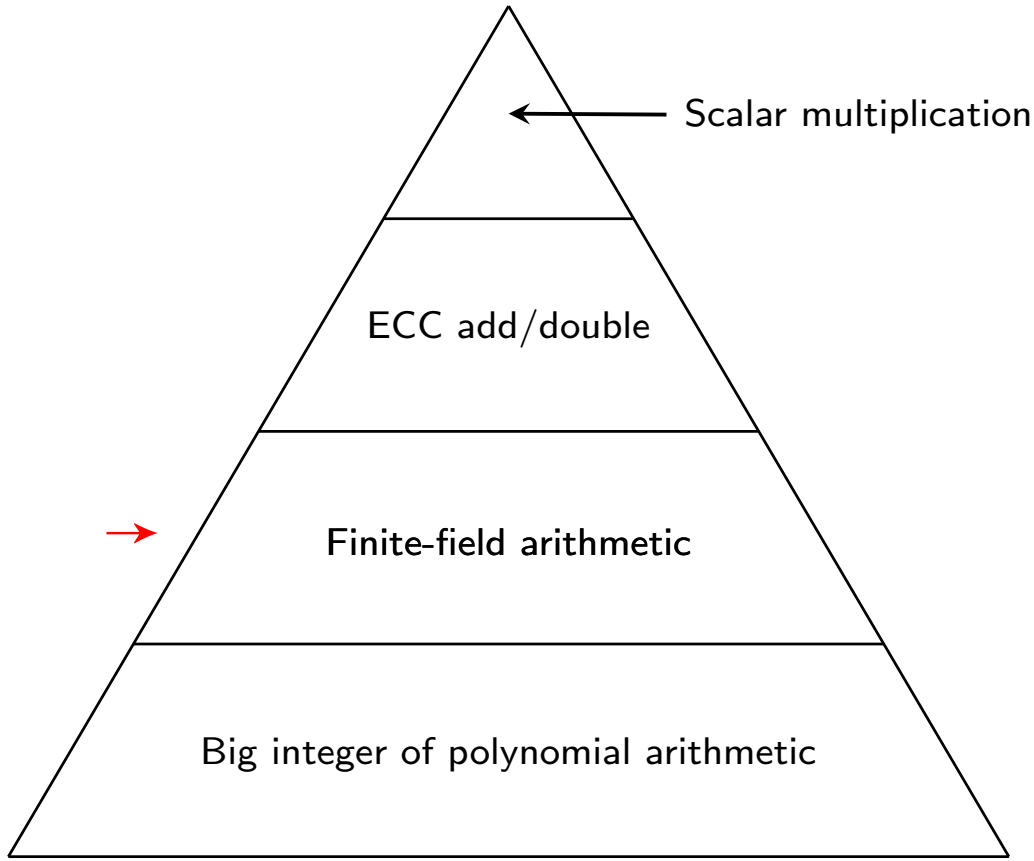

Scalar multiplication
ECC add/double
Finite-field arithmetic
Big integer of polynomial arithmetic

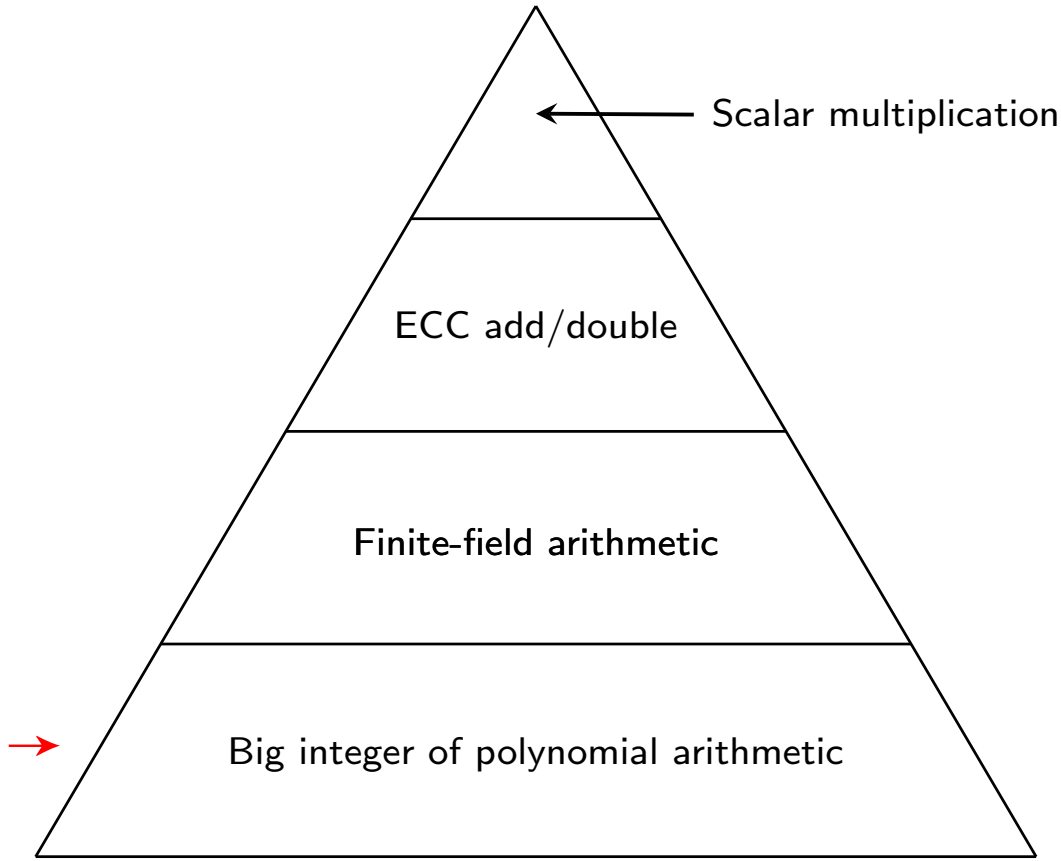
Montgomery ladder step

$$A = X_2 + Z_2$$
$$AA = A^2$$
$$B = X_2 - Z_2$$
$$BB = B^2$$
$$E = AA - BB$$
$$C = X_3 + Z_3$$
$$D = X_3 - Z_3$$
$$DA = D * A$$
$$CB = C * B$$
$$X_5 = Z_1 * (DA + CB)^2$$
$$Z_5 = X_1 * (DA - CB)^2$$
$$X_4 = AA * BB$$
$$Z_4 = E * (BB + a_{24} * E)$$

Doubling formula for twisted Edwards curves ($a = -1$)

$$
\begin{aligned}
A &= X_1^2 \\
B &= Y_1^2 \\
C &= 2 * Z_1^2 \\
D &= -A \\
E &= (X_1 + Y_1)^2 - A - B \\
G &= D + B \\
F &= G - C \\
H &= D - B \\
X_3 &= E * F \\
Y_3 &= G * H \\
Z_3 &= F * G
\end{aligned}
$$


Scalar multiplication
ECC add/double
Finite-field arithmetic
Big integer of polynomial arithmetic


Scalar multiplication
ECC add/double
Finite-field arithmetic
Big integer of polynomial arithmetic

Vectorizing one field multiplication

$$
\begin{aligned}
h_0 = {} & f_0g_0 + 38f_1g_9 + 19f_2g_8 + 38f_3g_7 + 19f_4g_6 + 38f_5g_5 + 19f_6g_4 + 38f_7g_3 + 19f_8g_2 + 38f_9g_1 \\
h_1 = {} & f_0g_1 + f_1g_0 + 19f_2g_9 + 19f_3g_8 + 19f_4g_7 + 19f_5g_6 + 19f_6g_5 + 19f_7g_4 + 19f_8g_3 + 19f_9g_2 \\
h_2 = {} & f_0g_2 + 2f_1g_1 + f_2g_0 + 38f_3g_9 + 19f_4g_8 + 38f_5g_7 + 19f_6g_6 + 38f_7g_5 + 19f_8g_4 + 38f_9g_3 \\
h_3 = {} & f_0g_3 + f_1g_2 + f_2g_1 + f_3g_0 + 19f_4g_9 + 19f_5g_8 + 19f_6g_7 + 19f_7g_6 + 19f_8g_5 + 19f_9g_4 \\
h_4 = {} & f_0g_4 + 2f_1g_3 + f_2g_2 + 2f_3g_1 + f_4g_0 + 38f_5g_9 + 19f_6g_8 + 38f_7g_7 + 19f_8g_6 + 38f_9g_5 \\
h_5 = {} & f_0g_5 + f_1g_4 + f_2g_3 + f_3g_2 + f_4g_1 + f_5g_0 + 19f_6g_9 + 19f_7g_8 + 19f_8g_7 + 19f_9g_6 \\
h_6 = {} & f_0g_6 + 2f_1g_5 + f_2g_4 + 2f_3g_3 + f_4g_2 + 2f_5g_1 + f_6g_0 + 38f_7g_9 + 19f_8g_8 + 38f_9g_7 \\
h_7 = {} & f_0g_7 + f_1g_6 + f_2g_5 + f_3g_4 + f_4g_3 + f_5g_2 + f_6g_1 + f_7g_0 + 19f_8g_9 + 19f_9g_8 \\
h_8 = {} & f_0g_8 + 2f_1g_7 + f_2g_6 + 2f_3g_5 + f_4g_4 + 2f_5g_3 + f_6g_2 + 2f_7g_1 + f_8g_0 + 38f_9g_9 \\
h_9 = {} & f_0g_9 + f_1g_8 + f_2g_7 + f_3g_6 + f_4g_5 + f_5g_4 + f_6g_3 + f_7g_2 + f_8g_1 + f_9g_0
\end{aligned}
$$

Vectorizing one field multiplication

$$
\begin{aligned}
h_0 = {} & f_0g_0 + 38f_1g_9 + 19f_2g_8 + 38f_3g_7 + 19f_4g_6 + 38f_5g_5 + 19f_6g_4 + 38f_7g_3 + 19f_8g_2 + 38f_9g_1 \\
h_1 = {} & f_0g_1 + f_1g_0 + 19f_2g_9 + 19f_3g_8 + 19f_4g_7 + 19f_5g_6 + 19f_6g_5 + 19f_7g_4 + 19f_8g_3 + 19f_9g_2 \\
h_2 = {} & f_0g_2 + 2f_1g_1 + f_2g_0 + 38f_3g_9 + 19f_4g_8 + 38f_5g_7 + 19f_6g_6 + 38f_7g_5 + 19f_8g_4 + 38f_9g_3 \\
h_3 = {} & f_0g_3 + f_1g_2 + f_2g_1 + f_3g_0 + 19f_4g_9 + 19f_5g_8 + 19f_6g_7 + 19f_7g_6 + 19f_8g_5 + 19f_9g_4 \\
h_4 = {} & f_0g_4 + 2f_1g_3 + f_2g_2 + 2f_3g_1 + f_4g_0 + 38f_5g_9 + 19f_6g_8 + 38f_7g_7 + 19f_8g_6 + 38f_9g_5 \\
h_5 = {} & f_0g_5 + f_1g_4 + f_2g_3 + f_3g_2 + f_4g_1 + f_5g_0 + 19f_6g_9 + 19f_7g_8 + 19f_8g_7 + 19f_9g_6 \\
h_6 = {} & f_0g_6 + 2f_1g_5 + f_2g_4 + 2f_3g_3 + f_4g_2 + 2f_5g_1 + f_6g_0 + 38f_7g_9 + 19f_8g_8 + 38f_9g_7 \\
h_7 = {} & f_0g_7 + f_1g_6 + f_2g_5 + f_3g_4 + f_4g_3 + f_5g_2 + f_6g_1 + f_7g_0 + 19f_8g_9 + 19f_9g_8 \\
h_8 = {} & f_0g_8 + 2f_1g_7 + f_2g_6 + 2f_3g_5 + f_4g_4 + 2f_5g_3 + f_6g_2 + 2f_7g_1 + f_8g_0 + 38f_9g_9 \\
h_9 = {} & f_0g_9 + f_1g_8 + f_2g_7 + f_3g_6 + f_4g_5 + f_5g_4 + f_6g_3 + f_7g_2 + f_8g_1 + f_9g_0
\end{aligned}
$$

Vectorizing one field multiplication

$$
\begin{array}{lllllllllll}
h_0 = & f_0g_0+ & 38f_1g_9+ & 19f_2g_8+ & 38f_3g_7+ & 19f_4g_6+ & 38f_5g_5+ & 19f_6g_4+ & 38f_7g_3+ & 19f_8g_2+ & 38f_9g_1 \\
h_1 = & f_0g_1+ & f_1g_0+ & 19f_2g_9+ & 19f_3g_8+ & 19f_4g_7+ & 19f_5g_6+ & 19f_6g_5+ & 19f_7g_4+ & 19f_8g_3+ & 19f_9g_2 \\
h_2 = & f_0g_2+ & 2f_1g_1+ & f_2g_0+ & 38f_3g_9+ & 19f_4g_8+ & 38f_5g_7+ & 19f_6g_6+ & 38f_7g_5+ & 19f_8g_4+ & 38f_9g_3 \\
h_3 = & f_0g_3+ & f_1g_2+ & f_2g_1+ & f_3g_0+ & 19f_4g_9+ & 19f_5g_8+ & 19f_6g_7+ & 19f_7g_6+ & 19f_8g_5+ & 19f_9g_4 \\
h_4 = & f_0g_4+ & 2f_1g_3+ & f_2g_2+ & 2f_3g_1+ & f_4g_0+ & 38f_5g_9+ & 19f_6g_8+ & 38f_7g_7+ & 19f_8g_6+ & 38f_9g_5 \\
h_5 = & f_0g_5+ & f_1g_4+ & f_2g_3+ & f_3g_2+ & f_4g_1+ & f_5g_0+ & 19f_6g_9+ & 19f_7g_8+ & 19f_8g_7+ & 19f_9g_6 \\
h_6 = & f_0g_6+ & 2f_1g_5+ & f_2g_4+ & 2f_3g_3+ & f_4g_2+ & 2f_5g_1+ & f_6g_0+ & 38f_7g_9+ & 19f_8g_8+ & 38f_9g_7 \\
h_7 = & f_0g_7+ & f_1g_6+ & f_2g_5+ & f_3g_4+ & f_4g_3+ & f_5g_2+ & f_6g_1+ & f_7g_0+ & 19f_8g_9+ & 19f_9g_8 \\
h_8 = & f_0g_8+ & 2f_1g_7+ & f_2g_6+ & 2f_3g_5+ & f_4g_4+ & 2f_5g_3+ & f_6g_2+ & 2f_7g_1+ & f_8g_0+ & 38f_9g_9 \\
h_9 = & f_0g_9+ & f_1g_8+ & f_2g_7+ & f_3g_6+ & f_4g_5+ & f_5g_4+ & f_6g_3+ & f_7g_2+ & f_8g_1+ & f_9g_0
\end{array}
$$

Vectorizing one field multiplication

$$
\begin{aligned}
h_0 = {} & f_0g_0 + 38f_1g_9 + 19f_2g_8 + 38f_3g_7 + 19f_4g_6 + 38f_5g_5 + 19f_6g_4 + 38f_7g_3 + 19f_8g_2 + 38f_9g_1 \\
h_1 = {} & f_0g_1 + f_1g_0 + 19f_2g_9 + 19f_3g_8 + 19f_4g_7 + 19f_5g_6 + 19f_6g_5 + 19f_7g_4 + 19f_8g_3 + 19f_9g_2 \\
h_2 = {} & f_0g_2 + 2f_1g_1 + f_2g_0 + 38f_3g_9 + 19f_4g_8 + 38f_5g_7 + 19f_6g_6 + 38f_7g_5 + 19f_8g_4 + 38f_9g_3 \\
h_3 = {} & f_0g_3 + f_1g_2 + f_2g_1 + f_3g_0 + 19f_4g_9 + 19f_5g_8 + 19f_6g_7 + 19f_7g_6 + 19f_8g_5 + 19f_9g_4 \\
h_4 = {} & f_0g_4 + 2f_1g_3 + f_2g_2 + 2f_3g_1 + f_4g_0 + 38f_5g_9 + 19f_6g_8 + 38f_7g_7 + 19f_8g_6 + 38f_9g_5 \\
h_5 = {} & f_0g_5 + f_1g_4 + f_2g_3 + f_3g_2 + f_4g_1 + f_5g_0 + 19f_6g_9 + 19f_7g_8 + 19f_8g_7 + 19f_9g_6 \\
h_6 = {} & f_0g_6 + 2f_1g_5 + f_2g_4 + 2f_3g_3 + f_4g_2 + 2f_5g_1 + f_6g_0 + 38f_7g_9 + 19f_8g_8 + 38f_9g_7 \\
h_7 = {} & f_0g_7 + f_1g_6 + f_2g_5 + f_3g_4 + f_4g_3 + f_5g_2 + f_6g_1 + f_7g_0 + 19f_8g_9 + 19f_9g_8 \\
h_8 = {} & f_0g_8 + 2f_1g_7 + f_2g_6 + 2f_3g_5 + f_4g_4 + 2f_5g_3 + f_6g_2 + 2f_7g_1 + f_8g_0 + 38f_9g_9 \\
h_9 = {} & f_0g_9 + f_1g_8 + f_2g_7 + f_3g_6 + f_4g_5 + f_5g_4 + f_6g_3 + f_7g_2 + f_8g_1 + f_9g_0
\end{aligned}
$$

Vectorizing one field multiplication

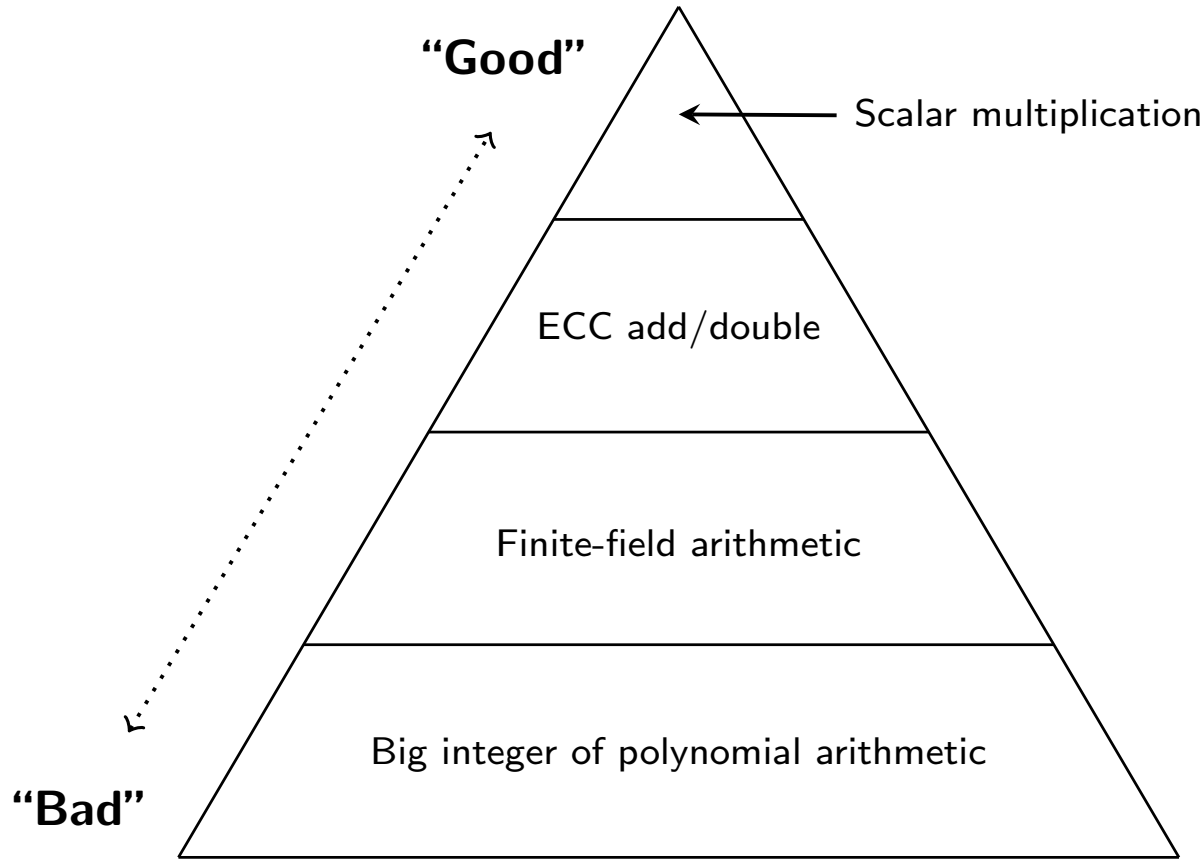
$$
\begin{aligned}
h_0 = {} & f_0g_0 + 38f_1g_9 + 19f_2g_8 + 38f_3g_7 + 19f_4g_6 + 38f_5g_5 + 19f_6g_4 + 38f_7g_3 + 19f_8g_2 + 38f_9g_1 \\
h_1 = {} & f_0g_1 + f_1g_0 + 19f_2g_9 + 19f_3g_8 + 19f_4g_7 + 19f_5g_6 + 19f_6g_5 + 19f_7g_4 + 19f_8g_3 + 19f_9g_2 \\
h_2 = {} & f_0g_2 + 2f_1g_1 + f_2g_0 + 38f_3g_9 + 19f_4g_8 + 38f_5g_7 + 19f_6g_6 + 38f_7g_5 + 19f_8g_4 + 38f_9g_3 \\
h_3 = {} & f_0g_3 + f_1g_2 + f_2g_1 + f_3g_0 + 19f_4g_9 + 19f_5g_8 + 19f_6g_7 + 19f_7g_6 + 19f_8g_5 + 19f_9g_4 \\
h_4 = {} & f_0g_4 + 2f_1g_3 + f_2g_2 + 2f_3g_1 + f_4g_0 + 38f_5g_9 + 19f_6g_8 + 38f_7g_7 + 19f_8g_6 + 38f_9g_5 \\
h_5 = {} & f_0g_5 + f_1g_4 + f_2g_3 + f_3g_2 + f_4g_1 + f_5g_0 + 19f_6g_9 + 19f_7g_8 + 19f_8g_7 + 19f_9g_6 \\
h_6 = {} & f_0g_6 + 2f_1g_5 + f_2g_4 + 2f_3g_3 + f_4g_2 + 2f_5g_1 + f_6g_0 + 38f_7g_9 + 19f_8g_8 + 38f_9g_7 \\
h_7 = {} & f_0g_7 + f_1g_6 + f_2g_5 + f_3g_4 + f_4g_3 + f_5g_2 + f_6g_1 + f_7g_0 + 19f_8g_9 + 19f_9g_8 \\
h_8 = {} & f_0g_8 + 2f_1g_7 + f_2g_6 + 2f_3g_5 + f_4g_4 + 2f_5g_3 + f_6g_2 + 2f_7g_1 + f_8g_0 + 38f_9g_9 \\
h_9 = {} & f_0g_9 + f_1g_8 + f_2g_7 + f_3g_6 + f_4g_5 + f_5g_4 + f_6g_3 + f_7g_2 + f_8g_1 + f_9g_0
\end{aligned}
$$

Vectorizing one field multiplication

$$
\begin{array}{rrrrrrrrrrr}
h_0 = & f_0g_0+ & 38f_1g_9+ & 19f_2g_8+ & 38f_3g_7+ & 19f_4g_6+ & 38f_5g_5+ & 19f_6g_4+ & 38f_7g_3+ & 19f_8g_2+ & 38f_9g_1 \\
h_1 = & f_0g_1+ & f_1g_0+ & 19f_2g_9+ & 19f_3g_8+ & 19f_4g_7+ & 19f_5g_6+ & 19f_6g_5+ & 19f_7g_4+ & 19f_8g_3+ & 19f_9g_2 \\
h_2 = & f_0g_2+ & 2f_1g_1+ & f_2g_0+ & 38f_3g_9+ & 19f_4g_8+ & 38f_5g_7+ & 19f_6g_6+ & 38f_7g_5+ & 19f_8g_4+ & 38f_9g_3 \\
h_3 = & f_0g_3+ & f_1g_2+ & f_2g_1+ & f_3g_0+ & 19f_4g_9+ & 19f_5g_8+ & 19f_6g_7+ & 19f_7g_6+ & 19f_8g_5+ & 19f_9g_4 \\
h_4 = & f_0g_4+ & 2f_1g_3+ & f_2g_2+ & 2f_3g_1+ & f_4g_0+ & 38f_5g_9+ & 19f_6g_8+ & 38f_7g_7+ & 19f_8g_6+ & 38f_9g_5 \\
h_5 = & f_0g_5+ & f_1g_4+ & f_2g_3+ & f_3g_2+ & f_4g_1+ & f_5g_0+ & 19f_6g_9+ & 19f_7g_8+ & 19f_8g_7+ & 19f_9g_6 \\
h_6 = & f_0g_6+ & 2f_1g_5+ & f_2g_4+ & 2f_3g_3+ & f_4g_2+ & 2f_5g_1+ & f_6g_0+ & 38f_7g_9+ & 19f_8g_8+ & 38f_9g_7 \\
h_7 = & f_0g_7+ & f_1g_6+ & f_2g_5+ & f_3g_4+ & f_4g_3+ & f_5g_2+ & f_6g_1+ & f_7g_0+ & 19f_8g_9+ & 19f_9g_8 \\
h_8 = & f_0g_8+ & 2f_1g_7+ & f_2g_6+ & 2f_3g_5+ & f_4g_4+ & 2f_5g_3+ & f_6g_2+ & 2f_7g_1+ & f_8g_0+ & 38f_9g_9 \\
h_9 = & f_0g_9+ & f_1g_8+ & f_2g_7+ & f_3g_6+ & f_4g_5+ & f_5g_4+ & f_6g_3+ & f_7g_2+ & f_8g_1+ & f_9g_0
\end{array}
$$

Carries are still tricky.

Message for the 1st part



Performance results

	SB cycles	IB cycles	reference
X25519 public-key generation	54 346	52 169	**Sandy2x**
	61 828	57 612	[A. Moon]
	194 165	182 876	[Ed25519]
X25519 shared secret computation	156 995	159 128	**Sandy2x**
	194 036	182 708	[Ed25519]
Ed25519 public-key generation	57 164	54 901	**Sandy2x**
	63 712	59 332	[A. Moon]
	64 015	61 099	[Ed25519]
Ed25519 sign	63 526	59 949	**Sandy2x**
	67 692	62 624	[A. Moon]
	72 444	67 284	[Ed25519]
Ed25519 verification	205 741	198 406	**Sandy2x**
	227 628	204 376	[A. Moon]
	222 564	209 060	[Ed25519]

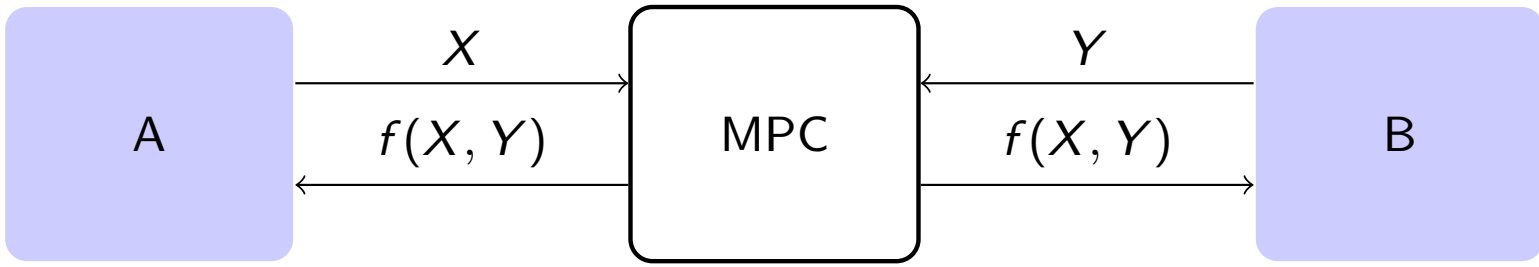
- Andrew Moon "floodyberry"

  `https://github.com/floodyberry/ed25519-donna`
- 256-bit registers?

  Armando Faz-Hernández, Julio López
  Fast Implementation of Curve25519 Using AVX2, Latincrypt 2015

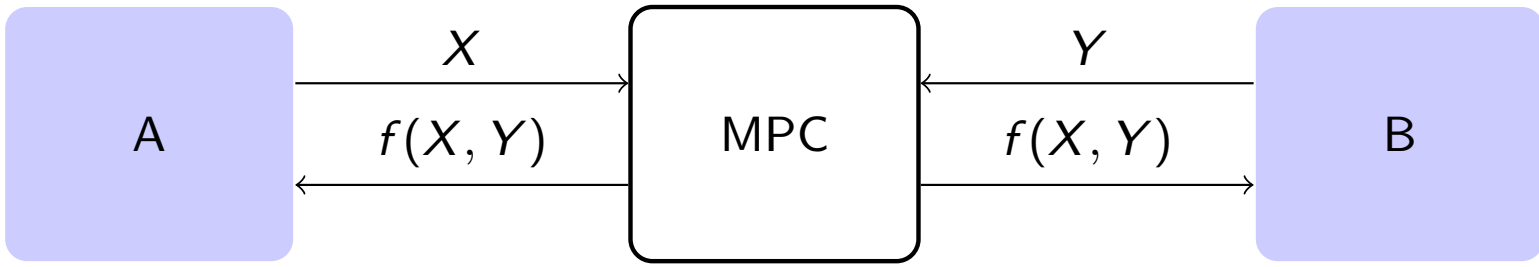
Part II.

Secure Multiparty Computation



The parties should learn no more than $f(X, Y)$

Secure Multiparty Computation



The parties should learn no more than $f(X, Y)$

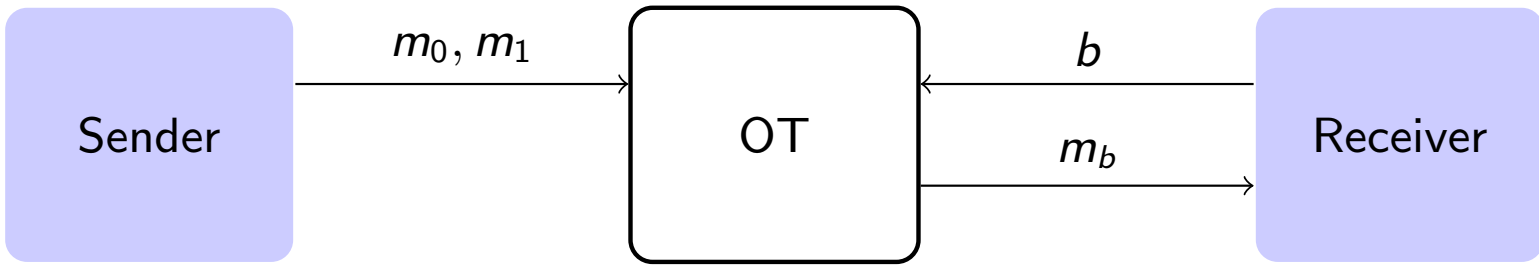
"OT is complete for secure multiparty computation."

$\binom{2}{1}$ OTs

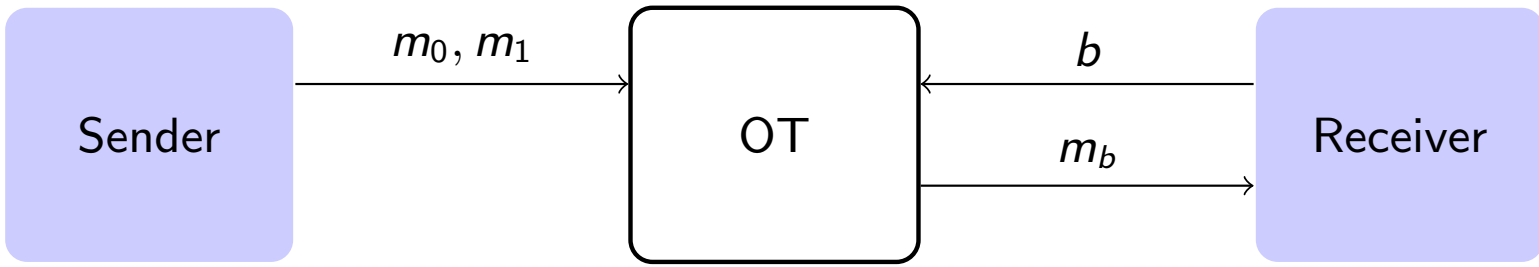
Sender

Receiver

$\binom{2}{1}$ OTs



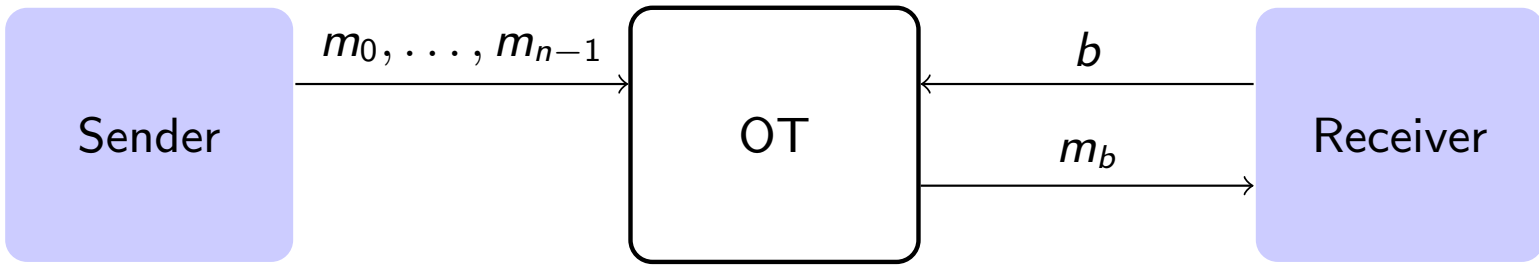
$\binom{2}{1}$ OTs



The **Receiver** should learn only m_b

The **Sender** should learn nothing

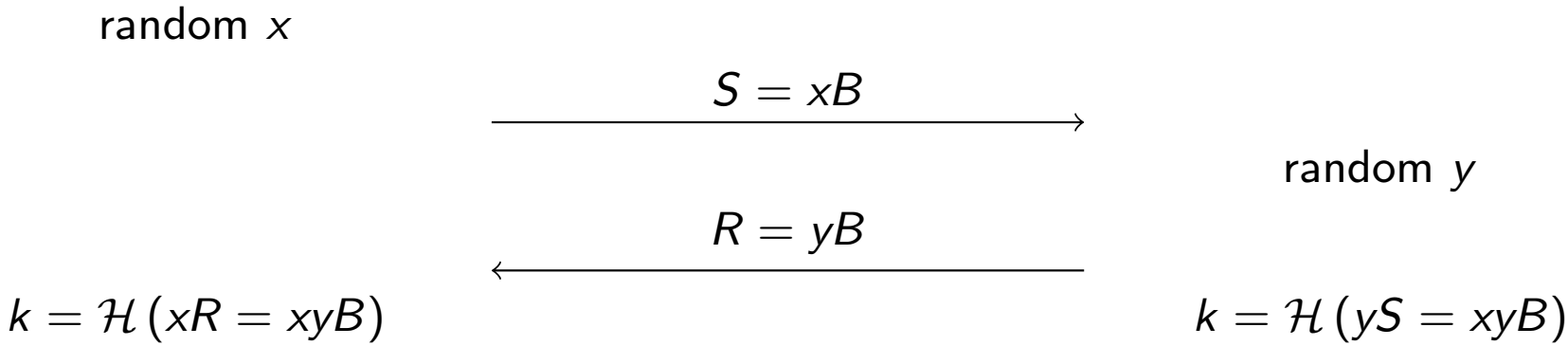
$\binom{n}{1}$ OTs



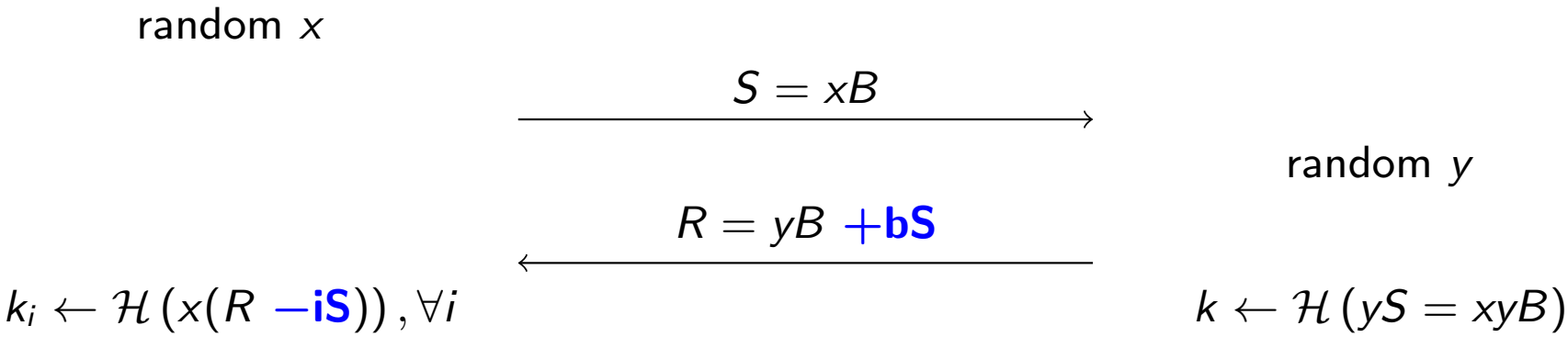
The **Receiver** should learn only m_b

The **Sender** should learn nothing

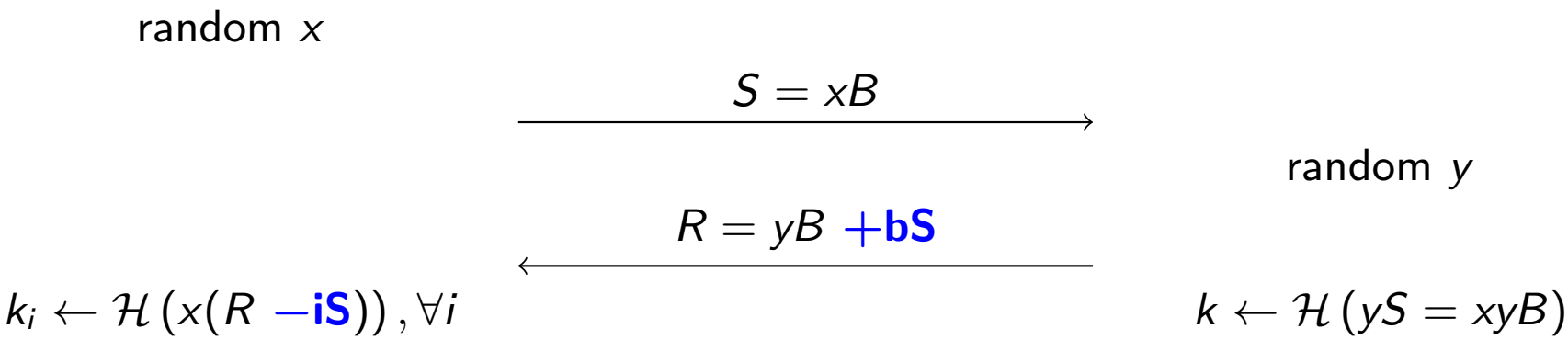
Diffie-Hellman



Our Random-OT construction

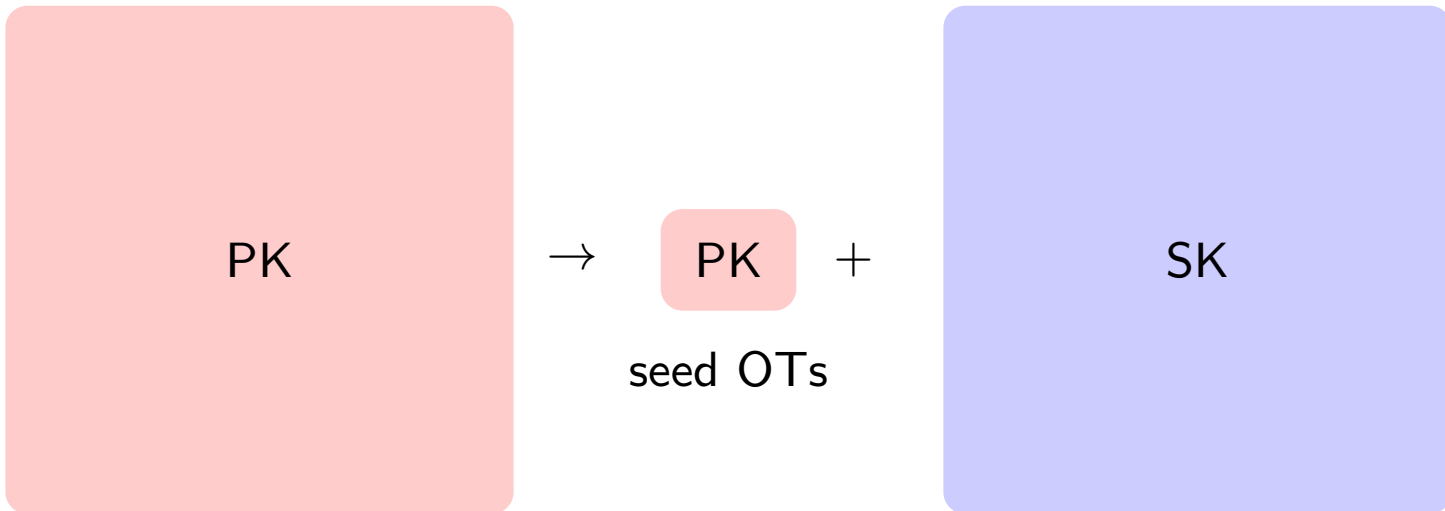


Our Random-OT construction



- R uniformly random: privacy for Receiver
- Square DH: privacy for Sender

OT Extension



- Similar to hybrid encryption
- Still we need base OTs

Experiment results

	m	64	128	256	512	1024
this work	Running time of $\mathcal{S}$	265	257	246	237	228
	Running time of $\mathcal{R}$	205	200	193	184	177
ALSZ13	Running time of $\mathcal{S}$	3348	2877	2650	2528	2473
	Running time of $\mathcal{R}$	3382	2909	2656	2541	2462

- ALSZ13: Gilad Asharov, Yehuda Lindell, Thomas Schneider, Michael Zohner, "More Efficient Oblivious Transfer and Extensions for Faster Secure Computation", 2013

Part 1:

www.win.tue.nl/~tchou/sandy2x/

Part 2:

users-cs.au.dk/orlandi/simpleOT/