qDSA: Small and Secure Digital Signatures with Curve-based Diffie-Hellman Key Pairs

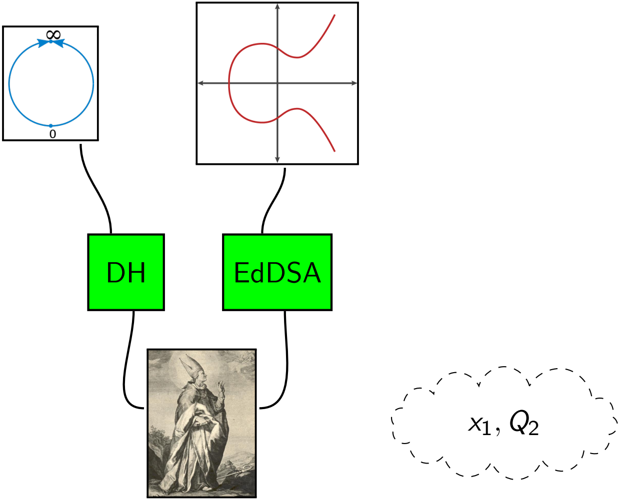
Joost Renes[1]   Benjamin Smith[2]

[1]Radboud University

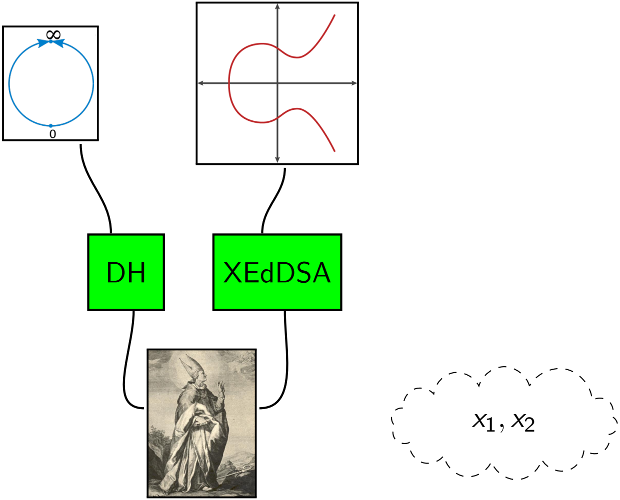
[2]INRIA *and* Laboratoire d'Informatique de l'École polytechnique

5 December 2017

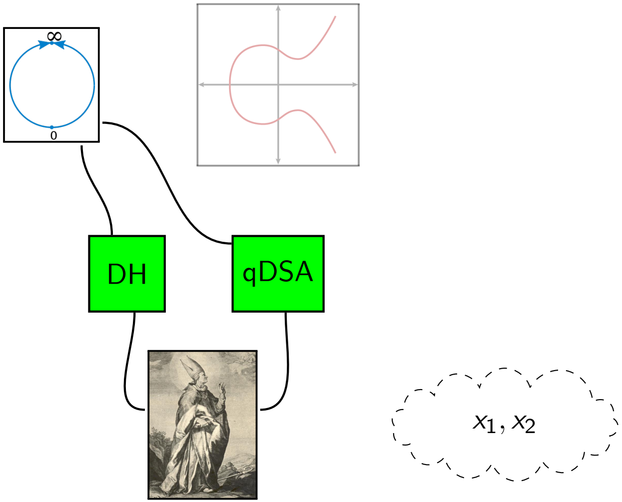
Curve-based crypto



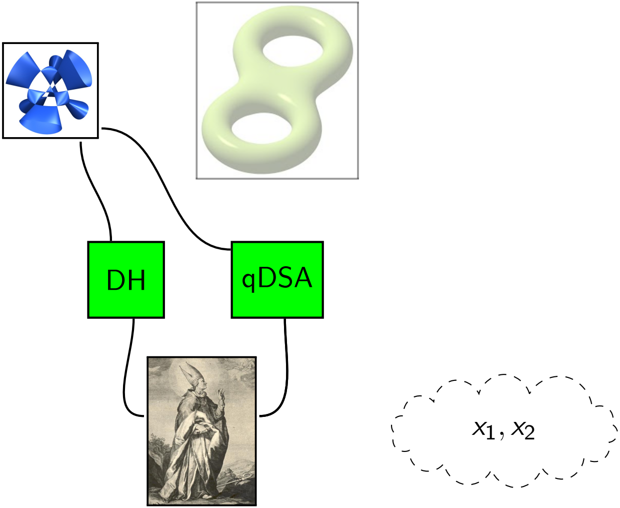
Curve-based crypto



Curve-based crypto



Curve-based crypto

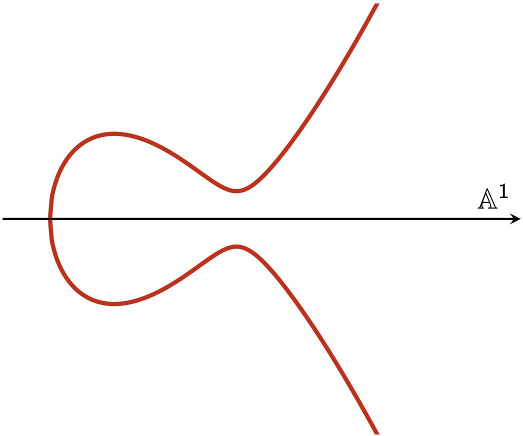


Operations on the Kummer line

Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

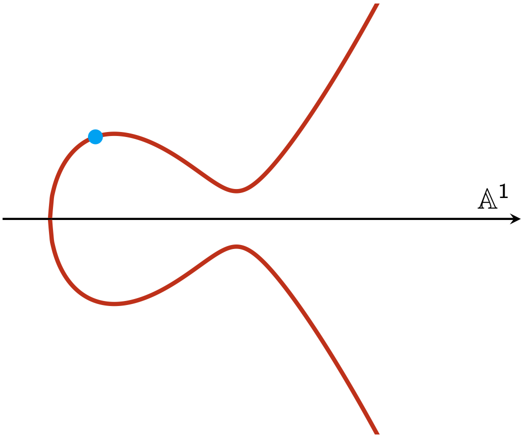


Operations on the Kummer line

Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

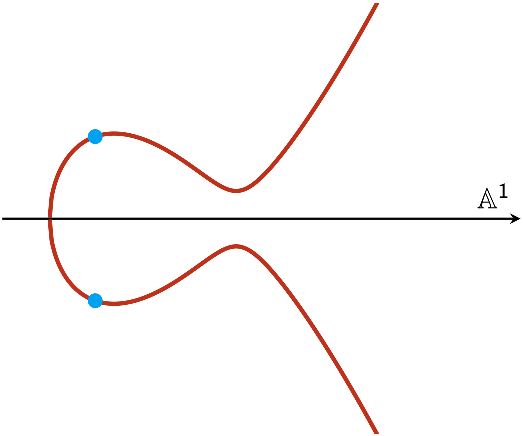


Operations on the Kummer line

Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

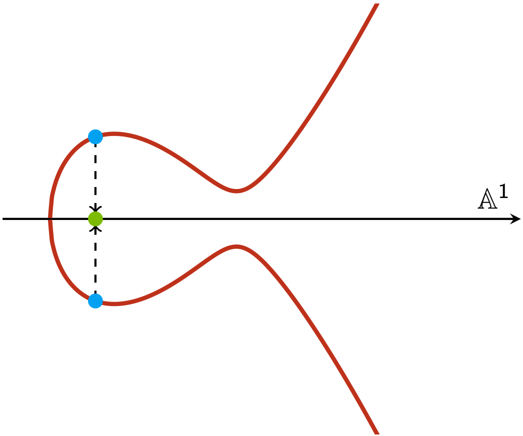


Operations on the Kummer line

Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

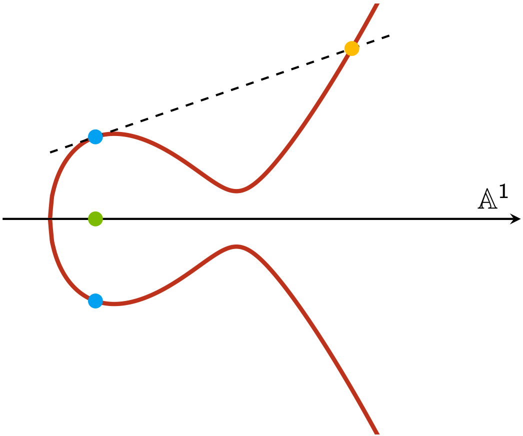


Operations on the Kummer line

Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

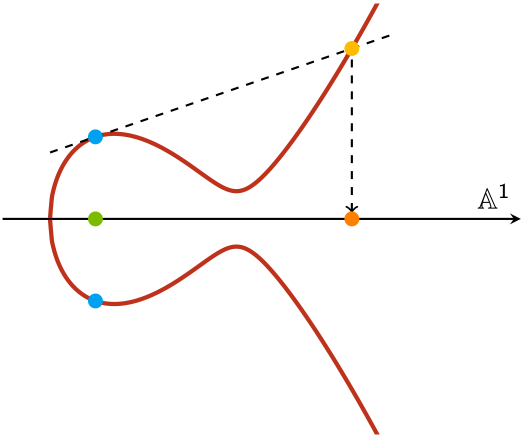


Operations on the Kummer line

Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

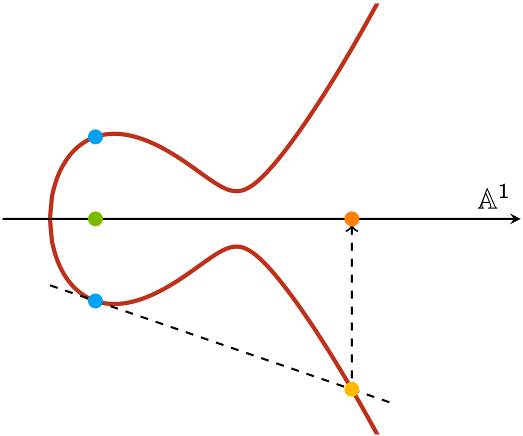


Operations on the Kummer line

Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$



Operations on the Kummer line

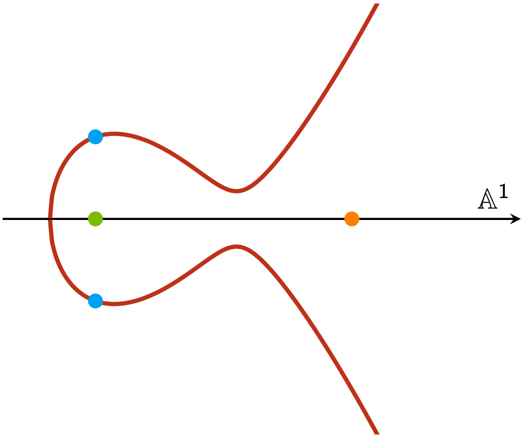
Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line

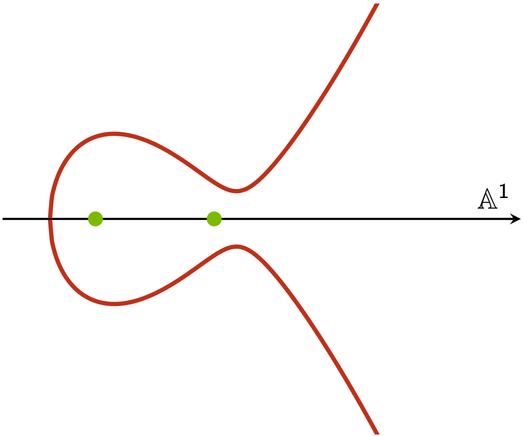
Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line

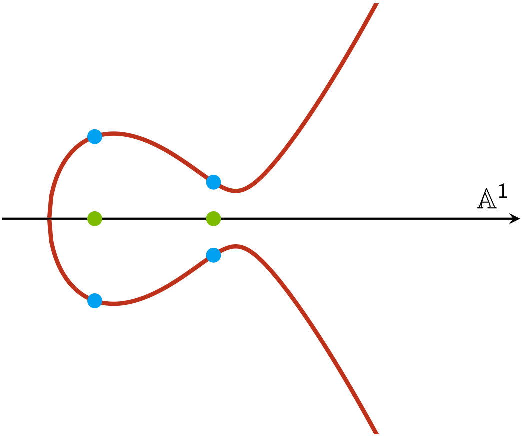
Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line

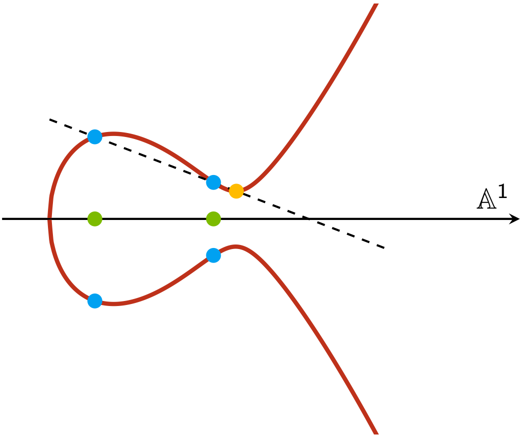
Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line

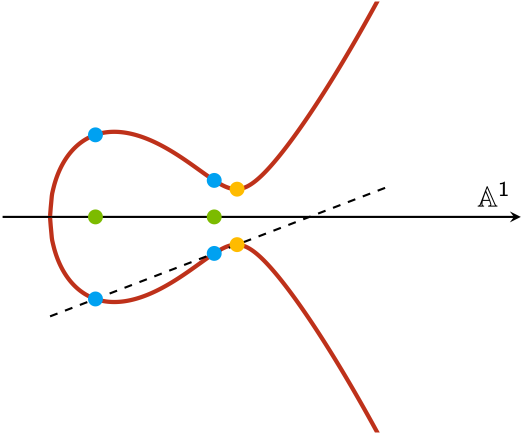
Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line

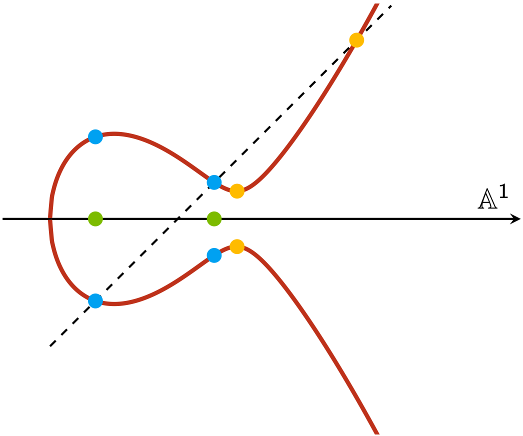
Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line

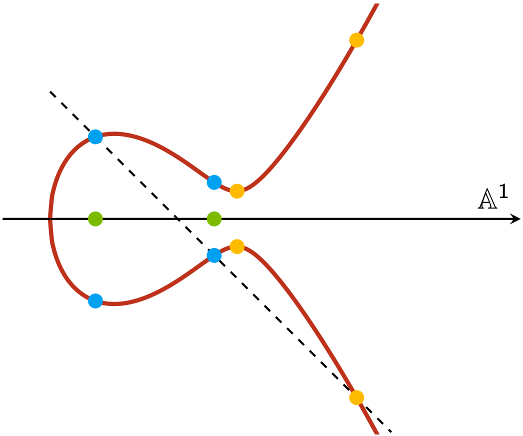
Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line

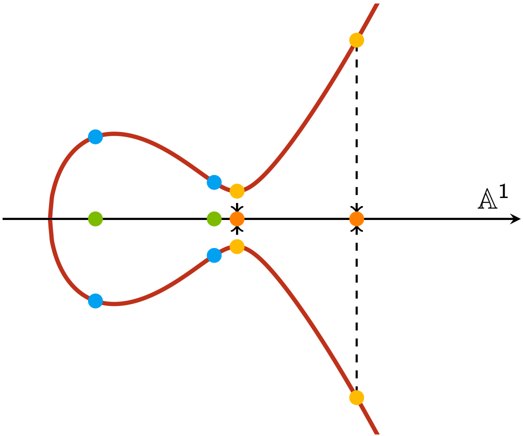
Operations on E

(1) $P \mapsto [2]P$

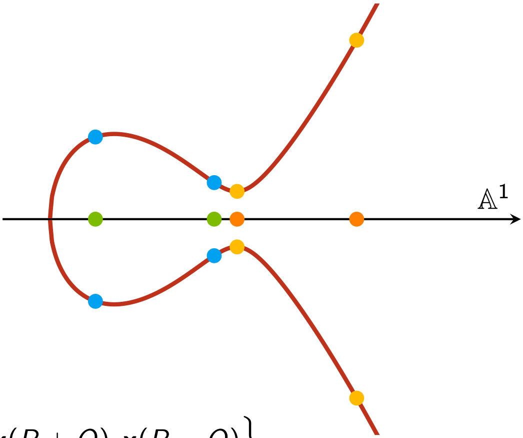
(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$



Operations on the Kummer line



Operations on E

(1) $P \mapsto [2]P$

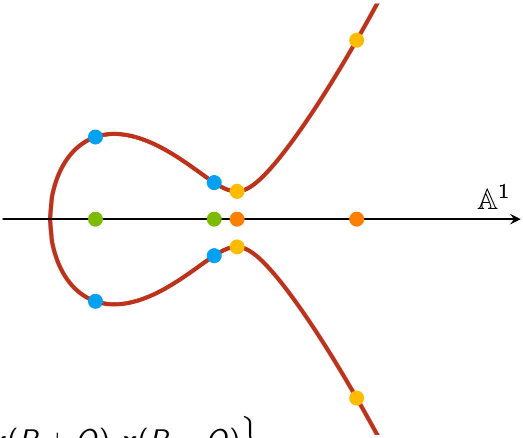
(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$

(2) $\left\{\mathbf{x}(P), \mathbf{x}(Q)\right\} \mapsto \left\{\mathbf{x}(P+Q), \mathbf{x}(P-Q)\right\}$

Operations on the Kummer line



Operations on E

(1) $P \mapsto [2]P$

(2) $\{P, Q\} \mapsto P + Q$

Operations on $\mathbb{P}^1$

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([2]P)$

(2) $\left\{\mathbf{x}(P), \mathbf{x}(Q)\right\} \mapsto \left\{\mathbf{x}(P+Q), \mathbf{x}(P-Q)\right\}$

$\implies \left\{\mathbf{x}(P), \mathbf{x}(Q), \mathbf{x}(P-Q)\right\} \mapsto \mathbf{x}(P+Q)$

Signatures on the Kummer

Starting point: Schnorr signatures [Sch89]

(1) Schnorr identification scheme (group-based)

(2) Apply Fiat-Shamir to make it non-interactive

(3) Include message to create a signature scheme

Signatures on the Kummer

Starting point: Schnorr signatures [Sch89]

(1) *Schnorr identification scheme (group-based)*

(2) Apply Fiat-Shamir to make it non-interactive

(3) Include message to create a signature scheme

Schnorr identification on the quotient (qID)

`Prover`(P, Q, α)	`Comm.`	`Verifier`(P, Q)

Schnorr identification on the quotient (qID)

$\texttt{Prover}(P, Q, \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(P, Q)$
$r \leftarrow_R \mathbb{Z}_N^*$		

Schnorr identification on the quotient (qID)

$\texttt{Prover}(P, Q, \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(P, Q)$
$r \leftarrow_R \mathbb{Z}_N^*$		
$R \leftarrow [r]P$	R	

Schnorr identification on the quotient (qID)

$\texttt{Prover}(P, Q, \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(P, Q)$
$r \leftarrow_R \mathbb{Z}_N^*$		
$R \leftarrow [r]P$	R	
	c	$c \leftarrow_R \mathbb{Z}_N$

Schnorr identification on the quotient (qID)

$\texttt{Prover}(P, Q, \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(P, Q)$
$r \leftarrow_R \mathbb{Z}_N^*$		
$R \leftarrow [r]P$	R	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	

Schnorr identification on the quotient (qID)

Prover(P, Q, α)	Comm.	Verifier(P, Q)
$r \leftarrow_R \mathbb{Z}_N^*$		
$R \leftarrow [r]P$	R	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	
		$R \stackrel{?}{=} [s]P + [c]Q$

Schnorr identification on the quotient (qID)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(\mathbf{x}(P), \mathbf{x}(Q))$
$r \leftarrow_R \mathbb{Z}_N^*$		
$R \leftarrow [r]P$	R	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	
		$R \stackrel{?}{=} [s]P + [c]Q$

Schnorr identification on the quotient (qID)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(\mathbf{x}(P), \mathbf{x}(Q))$
$r \leftarrow_R \mathbb{Z}_N^*$		
$\mathbf{x}(R) \leftarrow \mathbf{x}([r]P)$	$\mathbf{x}(R)$	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	
		$R \stackrel{?}{=} [s]P + [c]Q$

Schnorr identification on the quotient (qID)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(\mathbf{x}(P), \mathbf{x}(Q))$
$r \leftarrow_R \mathbb{Z}_N^*$		
$\mathbf{x}(R) \leftarrow \mathbf{x}([r]P)$	$\mathbf{x}(R)$	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	
		$R \stackrel{?}{=} [s]P + [c]Q$

Schnorr identification on the quotient (qID)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(\mathbf{x}(P), \mathbf{x}(Q))$
$r \leftarrow_R \mathbb{Z}_N^*$		
$\mathbf{x}(R) \leftarrow \mathbf{x}([r]P)$	$\mathbf{x}(R)$	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	
		$\mathbf{x}(R) \stackrel{?}{=} \mathbf{x}([s]P + [c]Q)$

Schnorr identification on the quotient (qID)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	$\texttt{Comm.}$	$\texttt{Verifier}(\mathbf{x}(P), \mathbf{x}(Q))$
$r \leftarrow_R \mathbb{Z}_N^*$		
$\mathbf{x}(R) \leftarrow \mathbf{x}([r]P)$	$\mathbf{x}(R)$	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	
		$\mathbf{x}(R) \stackrel{?}{=} \mathbf{x}([s]P \pm [c]Q)$

Schnorr identification on the quotient (qID)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	Comm.	$\texttt{Verifier}(\mathbf{x}(P), \mathbf{x}(Q))$
$r \leftarrow_R \mathbb{Z}_N^*$		
$\mathbf{x}(R) \leftarrow \mathbf{x}([r]P)$	$\mathbf{x}(R)$	
	c	$c \leftarrow_R \mathbb{Z}_N$
$s \leftarrow (r - c \cdot \alpha) \bmod N$	s	
		$\mathbf{x}(R) \stackrel{?}{=} \mathbf{x}([s]P \pm [c]Q)$

Need $\left\{\mathbf{x}(T_0 + T_1), \mathbf{x}(T_0 - T_1)\right\}$, where $T_0 = [s]P$ and $T_1 = [c]Q$

qSIG and qDSA

$$\underset{\text{(Schn. ID)}}{\text{qID}} \overset{\textit{Fiat-Shamir}}{\Longrightarrow} \underset{\text{(Schn. sig.)}}{\text{qSIG}}$$

qSIG and qDSA

$$\begin{array}{ccccc} \text{qID} & \overset{\textit{Fiat-Shamir}}{\Longrightarrow} & \text{qSIG} & \Longrightarrow & \text{qDSA} \\ \text{(Schn. ID)} & & \text{(Schn. sig.)} & & \text{(EdDSA)} \end{array}$$

qSIG and qDSA

$$\begin{matrix} \text{qID} \\ \text{(Schn. ID)} \end{matrix} \overset{\textit{Fiat-Shamir}}{\Longrightarrow} \begin{matrix} \text{qSIG} \\ \text{(Schn. sig.)} \end{matrix} \Longrightarrow \begin{matrix} \text{qDSA} \\ \text{(EdDSA)} \end{matrix}$$

(1) **Security reduction.** Similar to original Schnorr ID scheme

qSIG and qDSA

qID (Schn. ID)	$\overset{\textit{Fiat-Shamir}}{\Longrightarrow}$	qSIG (Schn. sig.)	$\Longrightarrow$	qDSA (EdDSA)

(1) **Security reduction.** Similar to original Schnorr ID scheme

(2) **Unified keys.** Identical key pairs for DH and qDSA

qSIG and qDSA

$$\begin{array}{ccccc} \text{qID} & \overset{\textit{Fiat-Shamir}}{\Longrightarrow} & \text{qSIG} & \Longrightarrow & \text{qDSA} \\ \text{(Schn. ID)} & & \text{(Schn. sig.)} & & \text{(EdDSA)} \end{array}$$

(1) **Security reduction.** Similar to original Schnorr ID scheme

(2) **Unified keys.** Identical key pairs for DH and qDSA

(3) **Key and signatures sizes.** 32-byte keys, 64-byte signatures

qSIG and qDSA

$$\begin{array}{ccccc} \text{qID} & \xrightarrow{\textit{Fiat-Shamir}} & \text{qSIG} & \Longrightarrow & \text{qDSA} \\ \text{(Schn. ID)} & & \text{(Schn. sig.)} & & \text{(EdDSA)} \end{array}$$

(1) **Security reduction.** Similar to original Schnorr ID scheme

(2) **Unified keys.** Identical key pairs for DH and qDSA

(3) **Key and signatures sizes.** 32-byte keys, 64-byte signatures

(4) **Verification.** Two-dimensional scalar multiplication algorithms not available & no batching

qSIG and qDSA

$$\begin{array}{ccccc} \text{qID} & \overset{\textit{Fiat-Shamir}}{\Longrightarrow} & \text{qSIG} & \Longrightarrow & \text{qDSA} \\ \text{(Schn. ID)} & & \text{(Schn. sig.)} & & \text{(EdDSA)} \end{array}$$

(1) **Security reduction.** Similar to original Schnorr ID scheme

(2) **Unified keys.** Identical key pairs for DH and qDSA

(3) **Key and signatures sizes.** 32-byte keys, 64-byte signatures

(4) **Verification.** Two-dimensional scalar multiplication algorithms not available & no batching

(5) **Side-channels & faults.** Add countermeasures *depending on context* of implementation

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\Big\{\mathbf{x}(P), \mathbf{x}(Q)\Big\} \mapsto \Big\{\mathbf{x}(P+Q), \mathbf{x}(P-Q)\Big\}$$

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\Big\{(X_1 : Z_1), (X_2 : Z_2)\Big\} \mapsto \Big\{(X_3 : Z_3), (X_4 : Z_4)\Big\}$$

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\left\{(X_1 : Z_1), (X_2 : Z_2)\right\} \mapsto \left\{(X_3 : Z_3), (X_4 : Z_4)\right\}$$

$$\left.\begin{aligned} X_3 X_4 &= B_{00}\,, \quad B_{00} = \nu \cdot (X_1 X_2 - Z_1 Z_2)^2 \\ Z_3 Z_4 &= B_{11}\,, \quad B_{11} = \nu \cdot (X_1 Z_2 - X_2 Z_1)^2 \end{aligned}\right\} \textbf{xADD}$$

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\Big\{(X_1 : Z_1), (X_2 : Z_2)\Big\} \mapsto \Big\{(X_3 : Z_3), (X_4 : Z_4)\Big\}$$

$$\left.\begin{aligned} X_3 X_4 &= B_{00}\,, & B_{00} &= \nu \cdot (X_1 X_2 - Z_1 Z_2)^2 \\ Z_3 Z_4 &= B_{11}\,, & B_{11} &= \nu \cdot (X_1 Z_2 - X_2 Z_1)^2 \end{aligned}\right\} \textbf{xADD}$$

$$\begin{aligned} X_3 Z_4 + X_4 Z_3 &= B_{10}\,, \quad B_{10} = \nu \cdot \big[\,(X_1 Z_2 - X_2 Z_1)(X_1 Z_2 + X_2 Z_1) \\ &\qquad + 2 A X_1 X_2 Z_1 Z_2\big] \end{aligned}$$

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\left\{(X_1 : Z_1),(X_2 : Z_2)\right\} \mapsto \left\{(X_3 : Z_3),(X_4 : Z_4)\right\}$$

$$\left.\begin{aligned} X_3X_4 &= B_{00}\,, & B_{00} &= \nu\cdot(X_1X_2 - Z_1Z_2)^2 \\ Z_3Z_4 &= B_{11}\,, & B_{11} &= \nu\cdot(X_1Z_2 - X_2Z_1)^2 \end{aligned}\right\} \textbf{xADD}$$

$$X_3Z_4 + X_4Z_3 = B_{10}\,, \quad B_{10} = \nu\cdot\left[(X_1Z_2 - X_2Z_1)(X_1Z_2 + X_2Z_1) + 2AX_1X_2Z_1Z_2\right]$$

$$\begin{pmatrix} X_3X_4 & * \\ X_3Z_4 + X_4Z_3 & Z_3Z_4 \end{pmatrix} = \nu\cdot\begin{pmatrix} B_{00} & * \\ B_{10} & B_{11} \end{pmatrix}$$

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\Big\{(X_1 : Z_1), (X_2 : Z_2)\Big\} \mapsto \Big\{(X_3 : Z_3), (X_4 : Z_4)\Big\}$$

$$\left.\begin{aligned} X_3X_4 &= B_{00}\,, & B_{00} &= \nu \cdot (X_1X_2 - Z_1Z_2)^2 \\ Z_3Z_4 &= B_{11}\,, & B_{11} &= \nu \cdot (X_1Z_2 - X_2Z_1)^2 \end{aligned}\right\} \textbf{xADD}$$

$$\begin{aligned} X_3Z_4 + X_4Z_3 &= B_{10}\,, & B_{10} &= \nu \cdot \big[(X_1Z_2 - X_2Z_1)(X_1Z_2 + X_2Z_1) \\ &&&\quad + 2AX_1X_2Z_1Z_2\big] \end{aligned}$$

$$\begin{pmatrix} X_3X_4 & * \\ X_3Z_4 + X_4Z_3 & Z_3Z_4 \end{pmatrix} = \nu \cdot \begin{pmatrix} B_{00} & * \\ B_{10} & B_{11} \end{pmatrix}$$

Thus $(X_3 : Z_3)$ and $(X_4 : Z_4)$ are the **unique** solutions to

$$B_{11}X^2 - 2 \cdot B_{10}XZ + B_{00}Z^2 = 0$$

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\left\{(X_1 : Z_1), (X_2 : Z_2)\right\} \mapsto \left\{(X_3 : Z_3), (X_4 : Z_4)\right\}$$

$$\left.\begin{aligned} X_3X_4 &= B_{00}\,, & B_{00} &= \nu \cdot (X_1X_2 - Z_1Z_2)^2 \\ Z_3Z_4 &= B_{11}\,, & B_{11} &= \nu \cdot (X_1Z_2 - X_2Z_1)^2 \end{aligned}\right\} \textbf{xADD}$$

$$X_3Z_4 + X_4Z_3 = B_{10}\,, \quad B_{10} = \nu \cdot \big[\,(X_1Z_2 - X_2Z_1)(X_1Z_2 + X_2Z_1) + 2AX_1X_2Z_1Z_2\big]$$

$$\begin{pmatrix} X_3X_4 & * \\ X_3Z_4 + X_4Z_3 & Z_3Z_4 \end{pmatrix} = \nu \cdot \begin{pmatrix} B_{00} & * \\ B_{10} & B_{11} \end{pmatrix} \qquad \mathbf{(2 \times 2)}$$

Thus $(X_3 : Z_3)$ and $(X_4 : Z_4)$ are the **unique** solutions to

$$B_{11}X^2 - 2 \cdot B_{10}XZ + B_{00}Z^2 = 0 \qquad \textbf{(1 eqn)}$$

Biquadratic forms on $\mathbb{P}^1$ for Montgomery curves

$$\left\{(X_1 : Z_1), (X_2 : Z_2)\right\} \mapsto \left\{(X_3 : Z_3), (X_4 : Z_4)\right\}$$

$$\left.\begin{aligned} X_3X_4 &= B_{00}\,, & B_{00} &= \nu \cdot (X_1X_2 - Z_1Z_2)^2 \\ Z_3Z_4 &= B_{11}\,, & B_{11} &= \nu \cdot (X_1Z_2 - X_2Z_1)^2 \end{aligned}\right\} \textbf{xADD}$$

$$X_3Z_4 + X_4Z_3 = B_{10}\,, \quad B_{10} = \nu \cdot \left[(X_1Z_2 - X_2Z_1)(X_1Z_2 + X_2Z_1) + 2AX_1X_2Z_1Z_2 \right]$$

$$\begin{pmatrix} X_3X_4 & * \\ X_3Z_4 + X_4Z_3 & Z_3Z_4 \end{pmatrix} = \nu \cdot \begin{pmatrix} B_{00} & * \\ B_{10} & B_{11} \end{pmatrix} \qquad \mathbf{(4 \times 4)}$$

Thus $(X_3 : Z_3)$ and $(X_4 : Z_4)$ are the **unique** solutions to

$$B_{11}X^2 - 2 \cdot B_{10}XZ + B_{00}Z^2 = 0 \qquad \textbf{(6 eqns)}$$

Cost of computing biquadratic forms

g	**Func.**	**M**	**S**	**C**
1	`Check`	8	3	1
	`Ladder`	1 280	1 024	256
2	`Check`	76	8	88
	`Ladder`	1 799	3 072	3 072

Table: Cost of B_{IJ}

Implementing the scheme (at 128-bit security)

g.	Ref.	Object.	Function.	CC.	Stack.
	This	`Curve25519`	`sign`	14 M	512 B
1	[NLD15]	`Ed25519`	`sign`	19 M	1 473 B
	[Liu+17]	Four$\mathbb{Q}$	`sign`	5 M	1 572 B

Table: AVR ATmega comparison (rounded)

Implementing the scheme (at 128-bit security)

g.	Ref.	Object.	Function.	CC.	Stack.
	This	`Curve25519`	`verify`	25 M	644 B
1	[NLD15]	`Ed25519`	`verify`	31 M	1 226 B
	[Liu+17]	Four$\mathbb{Q}$	`verify`	11 M	4 957 B

Table: AVR ATmega comparison (rounded)

Implementing the scheme (at 128-bit security)

g.	Ref.	Object.	Function.	CC.	Stack.
2	**This**	`Gaudry-Schost`	`sign`	10 M	417 B
	[Ren+16]	`Gaudry-Schost`	`sign`	10 M	926 B

Table: AVR ATmega comparison (rounded)

Implementing the scheme (at 128-bit security)

g.	Ref.	Object.	Function.	CC.	Stack.
2	**This**	`Gaudry-Schost`	`verify`	20 M	609 B
	[Ren+16]	`Gaudry-Schost`	`verify`	16 M	992 B

Table: AVR ATmega comparison (rounded)

Thanks for your attention!

`http://www.cs.ru.nl/~jrenes/`

References I

[Liu+17] Zhe Liu, Patrick Longa, Geovandro Pereira, Oscar Reparaz and Hwajeong Seo. *Four$\mathbb{Q}$ on embedded devices with strong countermeasures against side-channel attacks*. Cryptology ePrint Archive, Report 2017/434. http://eprint.iacr.org/2017/434. 2017.

[NLD15] Erick Nascimento, Julio López and Ricardo Dahab. "Efficient and Secure Elliptic Curve Cryptography for 8-bit AVR Microcontrollers". In: *Security, Privacy, and Applied Cryptography Engineering*. Ed. by Rajat Subhra Chakraborty, Peter Schwabe and Jon Solworth. Vol. 9354. LNCS. Springer, 2015, pp. 289–309.

[Ren+16] Joost Renes, Peter Schwabe, Benjamin Smith and Lejla Batina. "μKummer: Efficient Hyperelliptic Signatures and Key Exchange on Microcontrollers". In: *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*. 2016, pp. 301–320. DOI: 10.1007/978-3-662-53140-2_15. URL: http://dx.doi.org/10.1007/978-3-662-53140-2_15.

References II

[Sch89] Claus-Peter Schnorr. “Efficient Identification and Signatures for Smart Cards”. In: *Advances in Cryptology - CRYPTO ’89*. Ed. by Gilles Brassard. Vol. 435. LNCS. Springer, 1989, pp. 239–252.