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

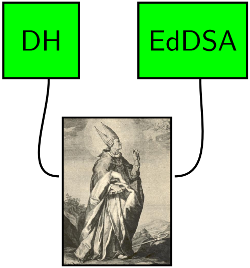
Joost Renes[1]   Benjamin Smith[2]

[1]Radboud University

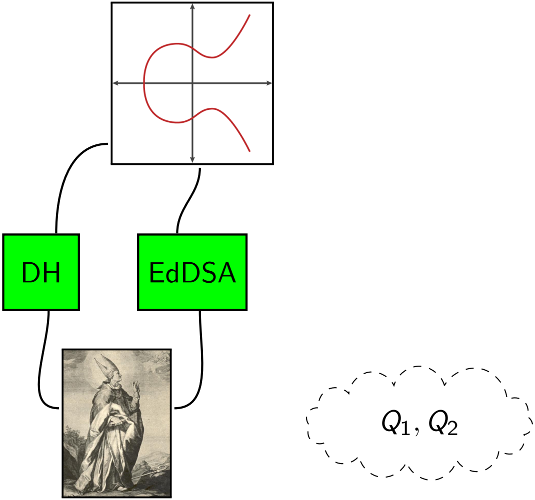
[2]INRIA *and* Laboratoire d'Informatique de l'École polytechnique

15 November 2017

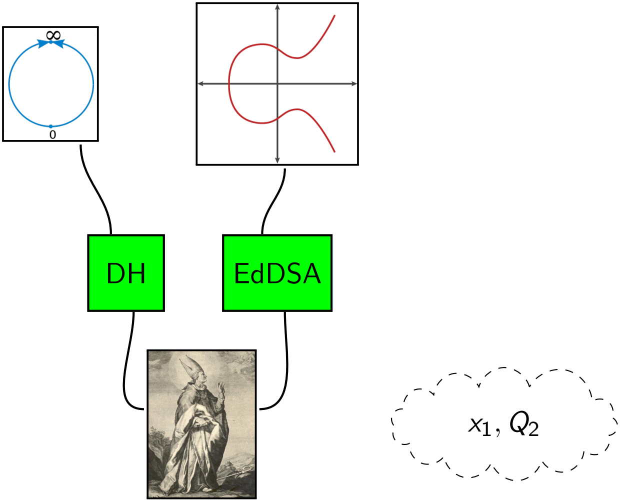
Curve-based crypto



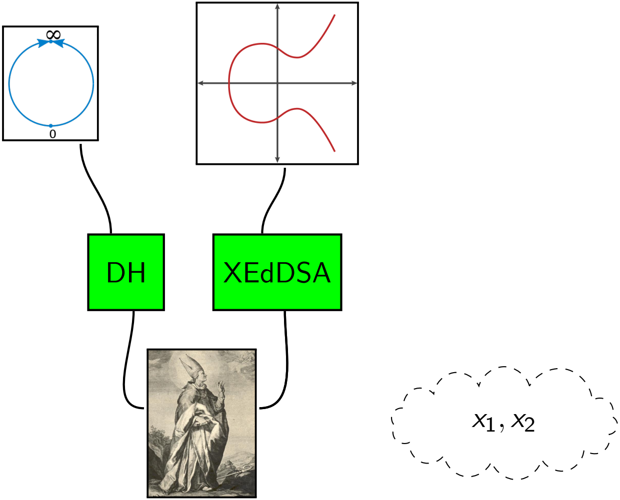
Curve-based crypto



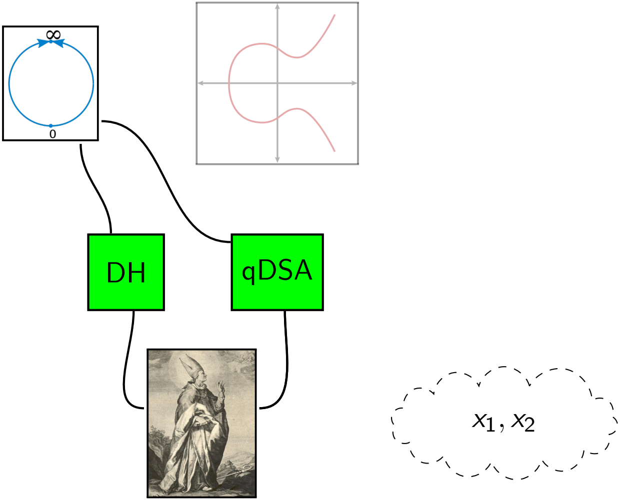
Curve-based crypto



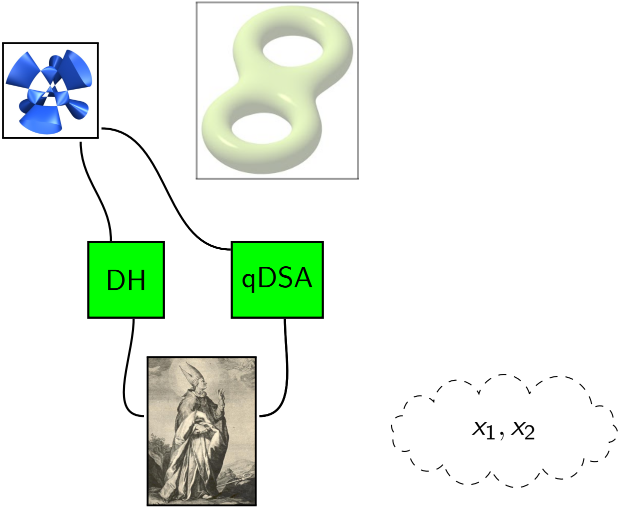
Curve-based crypto



Curve-based crypto



Curve-based crypto



Outline

(1) Quotient operations

(2) The qDSA scheme

(3) Instantiating with the x-line

(4) Instantiating with Kummer surfaces

Operations on quotient groups

$$G \longrightarrow G$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations on quotient groups

$$\begin{array}{ccc} G & \longrightarrow & G \\ \\ G/\pm 1 & \longrightarrow & G/\pm 1 \end{array}$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

Operations on quotient groups

$$\begin{tikzcd} G \arrow[r] & G \arrow[d] \\ G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 \end{tikzcd}$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

Operations on quotient groups

$$\begin{tikzcd} G \arrow[r] & G \arrow[d] \\ G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 \end{tikzcd}$$

$\mathbf{x}(P)$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

Operations on quotient groups

$$\begin{tikzcd}
\{P, -P\} & & \\
& G \arrow[r] & G \arrow[d] \\
& G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 \\
\mathbf{x}(P) \arrow[uuu, dashed, mapsto] & &
\end{tikzcd}$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

Operations on quotient groups

$$
\begin{tikzcd}
\{P,-P\} \arrow[rrr, dashed, mapsto] & & & \{[\lambda]P,-[\lambda]P\} \\
& G \arrow[r] & G \arrow[d] & \\
\mathbf{x}(P) \arrow[uu, dashed, mapsto] & G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 &
\end{tikzcd}
$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

Operations on quotient groups

$$
\begin{tikzcd}
\{P, -P\} \arrow[rrr, dashed, mapsto] & & & \{[\lambda]P, -[\lambda]P\} \arrow[ddd, dashed, mapsto] \\
& G \arrow[r] & G \arrow[d] & \\
& G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 & \\
\mathbf{x}(P) \arrow[uuu, dashed, mapsto] & & & \mathbf{x}([\lambda]P)
\end{tikzcd}
$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

Operations on quotient groups

$$
\begin{tikzcd}
\{P, -P\} \arrow[rrr, mapsto, dashed] & & & \{[\lambda]P, -[\lambda]P\} \arrow[ddd, mapsto, dashed] \\
& G \arrow[r] & G \arrow[d] & \\
& G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 & \\
\mathbf{x}(P) \arrow[uuu, mapsto, dashed] & & & \mathbf{x}([\lambda]P)
\end{tikzcd}
$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

(Q1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$

Operations on quotient groups

$$\begin{array}{ccc} G & \longrightarrow & G \\ \uparrow & & \downarrow \\ G/\pm 1 & \longrightarrow & G/\pm 1 \end{array}$$

$(\mathbf{x}(P), \mathbf{x}(Q))$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

(Q1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$

Operations on quotient groups

$$
\begin{tikzcd}
\{\{P,-P\},\{Q,-Q\}\} & & \\
& G \arrow[r] & G \arrow[d] \\
& G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 \\
(\mathbf{x}(P),\mathbf{x}(Q)) \arrow[uuu, dashed, mapsto] & &
\end{tikzcd}
$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

(Q1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$

Operations on quotient groups

$$
\begin{tikzcd}
\{\{P,-P\},\{Q,-Q\}\} \arrow[rr, mapsto, dashed] & & \{\pm(P \pm Q)\} \\
& G \arrow[r] & G \arrow[d] \\
& G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 \\
(\mathbf{x}(P),\mathbf{x}(Q)) \arrow[uuu, mapsto, dashed] & &
\end{tikzcd}
$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

(Q1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$

Operations on quotient groups

$$
\begin{tikzcd}
\{\{P,-P\},\{Q,-Q\}\} \arrow[rrr, dashed, mapsto] & & & \{\pm(P \pm Q)\} \arrow[ddd, dashed, mapsto] \\
& G \arrow[r] & G \arrow[d] & \\
& G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 & \\
(\mathbf{x}(P), \mathbf{x}(Q)) \arrow[uuu, dashed, mapsto] & & & \{\mathbf{x}(P \pm Q)\}
\end{tikzcd}
$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

(Q1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$

Operations on quotient groups

$$\begin{tikzcd}
\{\{P,-P\},\{Q,-Q\}\} \arrow[rrr, dashed, mapsto] & & & \{\pm(P \pm Q)\} \arrow[ddd, dashed, mapsto] \\
& G \arrow[r] & G \arrow[d] & \\
& G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 & \\
(\mathbf{x}(P),\mathbf{x}(Q)) \arrow[uuu, dashed, mapsto] & & & \{\mathbf{x}(P \pm Q)\}
\end{tikzcd}$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

(Q1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$

(Q2) $(\mathbf{x}(P), \mathbf{x}(Q)) \mapsto \{\mathbf{x}(P + Q), \mathbf{x}(P - Q)\}$

Operations on quotient groups

$$\begin{tikzcd} G \arrow[r] & G \arrow[d] \\ G/\pm 1 \arrow[u] \arrow[r] & G/\pm 1 \end{tikzcd}$$

Operations $G \to G$

(G1) $P \mapsto [\lambda]P$

(G2) $(P, Q) \mapsto P + Q$

Operations $G/\pm 1 \to G/\pm 1$

(Q1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$

(Q2) $(\mathbf{x}(P), \mathbf{x}(Q)) \mapsto \{\mathbf{x}(P + Q), \mathbf{x}(P - Q)\}$

Schnorr signatures

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 signatures

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)

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

Schnorr identification on the quotient (qID)

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

Schnorr identification on the quotient (qID)

$\texttt{Prover}(P, Q, \alpha)$	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)

$\texttt{Prover}(P, Q, \alpha)$	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)

$\texttt{Prover}(P, Q, \alpha)$	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	
		$R \stackrel{?}{=} [s]P + [c]Q$

Schnorr identification on the quotient (qID)

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

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	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)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	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)

$\texttt{Prover}(\mathbf{x}(P), \mathbf{x}(Q), \alpha)$	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	
		$\mathbf{x}(R) \overset{?}{\in} \{\mathbf{x}([s]P \pm [c]Q)\}$

Need $\{\mathbf{x}([s]P + [c]Q), \mathbf{x}([s]P - [c]Q)\}$.. possible on $G / \pm 1$!

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	
		$\mathbf{x}(R) \stackrel{?}{\in} \{\mathbf{x}([s]P \pm [c]Q)\}$

Need $\{\mathbf{x}([s]P + [c]Q), \mathbf{x}([s]P - [c]Q)\}$.. possible on $G \,/\, \pm 1$!

qSIG and qDSA

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

qSIG and qDSA

(1) Include the public key in the challenge

(2) Generate ephemeral secret r pseudo-randomly

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

qSIG and qDSA

(1) Include the public key in the challenge

(2) Generate ephemeral secret r pseudo-randomly

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

Add countermeasures against side-channel attacks

qSIG and qDSA

(1) Include the public key in the challenge

(2) Generate ephemeral secret r pseudo-randomly

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

Add countermeasures against side-channel attacks

(3) Fault attacks on ephemeral scalar multiplication

- Add randomness into hash for nonce generation

qSIG and qDSA

(1) Include the public key in the challenge

(2) Generate ephemeral secret r pseudo-randomly

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

Add countermeasures against side-channel attacks

(3) Fault attacks on ephemeral scalar multiplication

- Add randomness into hash for nonce generation

(4) Fault attacks on base point (Mehdi's talk on Monday)

- Clamp, or add a small cofactor into the computation
- Verify correctness of base point

Additional remarks

(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 (requires work in genus 2!)

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

Back to curves

Here, G the Jacobian group of a hyperelliptic curve of genus g

- Elliptic curves for $g = 1$, have $\mathcal{J} \,/\, \pm 1 = \mathbb{P}^1$
- Hyperelliptic curves with $g = 2$, have $\mathcal{J} \,/\, \pm 1 = \mathcal{K}$
- For $g \geq 3$ does not scale well (index calculus)

Back to curves

Here, G the Jacobian group of a hyperelliptic curve of genus g

- Elliptic curves for $g = 1$, have $\mathcal{J} / \pm 1 = \mathbb{P}^1$
- Hyperelliptic curves with $g = 2$, have $\mathcal{J} / \pm 1 = \mathcal{K}$
- For $g \geq 3$ does not scale well (index calculus)

Need to define

(1) $\mathbf{x}(P) \mapsto \mathbf{x}([\lambda]P)$ (usual way via Montgomery ladder)

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

(3) For any $\mathbf{x}(P)$, a 32-byte representation of $\mathbf{x}(P)$

On the choice of model ($g = 1$)

For elliptic curves common choice of Montgomery model

$$E/\mathbb{F}_p : By^2 = x^3 + Ax^2 + x$$

We obtain `Curve25519` by defining

$$p = 2^{255} - 19\,, \quad A = 486662\,, \quad B = 1$$

Arithmetic on $\mathbb{P}^1$

If

$$\mathbf{x}(P) = (X_1 : Z_1)\,, \qquad \mathbf{x}(P+Q) = (X_3 : Z_3)\,,$$
$$\mathbf{x}(Q) = (X_2 : Z_2)\,, \qquad \mathbf{x}(P-Q) = (X_4 : Z_4)\,,$$

then

$$\texttt{xADD}: \begin{array}{l} X_3X_4 = \lambda \cdot (X_1X_2 - Z_1Z_2)^2 \;, \\ Z_3Z_4 = \lambda \cdot (X_1Z_2 - X_2Z_1)^2 \;, \end{array}$$

Arithmetic on $\mathbb{P}^1$

If

$$\mathbf{x}(P) = (X_1 : Z_1)\,, \qquad \mathbf{x}(P+Q) = (X_3 : Z_3)\,,$$
$$\mathbf{x}(Q) = (X_2 : Z_2)\,, \qquad \mathbf{x}(P-Q) = (X_4 : Z_4)\,,$$

then

$$\texttt{xADD}: \begin{array}{l} X_3X_4 = \lambda \cdot (X_1X_2 - Z_1Z_2)^2\,, \\ Z_3Z_4 = \lambda \cdot (X_1Z_2 - X_2Z_1)^2\,, \end{array}$$

$$\texttt{xDBL}: \begin{array}{l} X_3 = \mu \cdot \left(X^2 - Z^2\right)^2\,, \\ Z_3 = \mu \cdot 4XZ\left(X^2 + AXZ + Z^2\right) \end{array}$$

Biquadratic forms on $\mathbb{P}^1$

In fact, have

$$\begin{aligned} X_3X_4 &= B_{00}\,, \quad & B_{00} &= \nu\cdot(X_1X_2 - Z_1Z_2)^2\,, \\ Z_3Z_4 &= B_{11}\,, \quad & B_{11} &= \nu\cdot(X_1Z_2 - X_2Z_1)^2\,, \\ X_3Z_4 + X_4Z_3 &= B_{10}\,, \quad & B_{10} &= \nu\cdot\big[(X_1Z_2 - X_2Z_1)(X_1Z_2 + X_2Z_1) \\ & & &\qquad + 2AX_1X_2Z_1Z_2\big]\,, \end{aligned}$$

Biquadratic forms on $\mathbb{P}^1$

In fact, have

$$\begin{aligned}
X_3X_4 = B_{00}\,, &\quad B_{00} = \nu \cdot (X_1X_2 - Z_1Z_2)^2\ , \\
Z_3Z_4 = B_{11}\,, &\quad B_{11} = \nu \cdot (X_1Z_2 - X_2Z_1)^2\ , \\
X_3Z_4 + X_4Z_3 = B_{10}\,, &\quad B_{10} = \nu \cdot \big[\,(X_1Z_2 - X_2Z_1)\,(X_1Z_2 + X_2Z_1) \\
&\qquad\qquad + 2AX_1X_2Z_1Z_2\big]\,,
\end{aligned}$$

ie.

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

Biquadratic forms on $\mathbb{P}^1$

In fact, have

$$\begin{aligned}
X_3X_4 = B_{00}\,, &\quad B_{00} = \nu\cdot(X_1X_2 - Z_1Z_2)^2\,,\\
Z_3Z_4 = B_{11}\,, &\quad B_{11} = \nu\cdot(X_1Z_2 - X_2Z_1)^2\,,\\
X_3Z_4 + X_4Z_3 = B_{10}\,, &\quad B_{10} = \nu\cdot\big[(X_1Z_2 - X_2Z_1)(X_1Z_2 + X_2Z_1)\\
&\qquad\qquad + 2AX_1X_2Z_1Z_2\big]\,,
\end{aligned}$$

ie.

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

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

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

Summarizing verification on $\mathbb{P}^1$

Given a signature $(\mathbf{x}(R) \mid\mid s)$ on M w.r.t. $\mathbf{x}(Q)$

(1) $c \leftarrow H(\mathbf{x}(R) \mid\mid M)$

(2) $\mathbf{x}(T_0) \leftarrow \mathbf{x}([s]P)$

(3) $\mathbf{x}(T_1) \leftarrow \mathbf{x}([c]Q)$

(4) Compute all B_{00}, B_{10}, B_{11} for $\mathbf{x}(T_0)$ and $\mathbf{x}(T_1)$

(5) Check that $\mathbf{x}(R)$ vanishes on

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

(*ie.* $\mathbf{x}(R) \in \{\mathbf{x}(T_0 + T_1), \mathbf{x}(T_0 - T_1)\}$)

On the choice of model ($g = 2$)

Gaudry-Schost curve [GS12]

$$
\begin{aligned}
\mathcal{E}/\mathbb{F}_{2^{127}-1} : y^2 = x^5 &+ 64408548613810695909971240431892164827 \cdot x^4 \\
&+ 76637216448498510246042731975843417626 \cdot x^3 \\
&+ 54735094972565041023366918099598639851 \cdot x^2 \\
&+ 98557324435909905133349189668472772222 \cdot x \\
&+ 81689052950067229064357938692912969725
\end{aligned}
$$

and its "squared" Kummer surface [CC86]

$$
\mathcal{K} : 4E^2 \cdot xyzt = \left(\begin{array}{c} x^2 + y^2 + z^2 + t^2 - F(xt + yz) \\ -G(xz + yt) - H(xy + zt) \end{array} \right)
$$

Arithmetic on $\mathcal{K}$

If

$$\mathbf{x}(P) = (x_1 : y_1 : z_1 : t_1)\,, \qquad \mathbf{x}(P+Q) = (x_3 : y_3 : z_3 : t_3)\,,$$
$$\mathbf{x}(Q) = (x_2 : y_2 : z_2 : t_2)\,, \qquad \mathbf{x}(P-Q) = (x_4 : y_4 : z_4 : t_4)\,,$$

then [Gau07; Ber+14]

$$\mathtt{xADD} : \begin{cases} x_3x_4 = \nu \cdot \varepsilon_1 \cdot (x' + y' + z' + t')^2\,, \\ y_3y_4 = \nu \cdot \varepsilon_2 \cdot (x' + y' - z' - t')^2\,, \\ z_3z_4 = \nu \cdot \varepsilon_3 \cdot (x' - y' + z' - t')^2\,, \\ t_3t_4 = \nu \cdot \varepsilon_4 \cdot (x' - y' - z' + t')^2\,, \text{ where} \\ \\ x' = \widehat{\varepsilon}_1 \cdot (x_1 + y_1 + z_1 + t_1) \cdot (x_2 + y_2 + z_2 + t_2) \\ y' = \widehat{\varepsilon}_2 \cdot (x_1 + y_1 - z_1 - t_1) \cdot (x_2 + y_2 - z_2 - t_2) \\ z' = \widehat{\varepsilon}_3 \cdot (x_1 - y_1 + z_1 - t_1) \cdot (x_2 - y_2 + z_2 - t_2) \\ t' = \widehat{\varepsilon}_4 \cdot (x_1 - y_1 - z_1 + t_1) \cdot (x_2 - y_2 - z_2 + t_2) \end{cases}$$

Quadratic identities on $\mathcal{K}$

These formulas give rise to an identity [Cos11]

$$\begin{pmatrix} 2x_3x_4 & * & * & * \\ * & 2y_3y_4 & * & * \\ * & * & 2z_3z_4 & * \\ * & * & * & 2t_3t_4 \end{pmatrix} = \nu \cdot \begin{pmatrix} B_{00} & * & * & * \\ * & B_{11} & * & * \\ * & * & B_{22} & * \\ * & * & * & B_{33} \end{pmatrix}$$

Quadratic identities on $\mathcal{K}$

These formulas give rise to an identity [Cos11]

$$\begin{pmatrix} 2x_3x_4 & * & * & * \\ \sigma(x,y) & 2y_3y_4 & * & * \\ \sigma(x,z) & \sigma(y,z) & 2z_3z_4 & * \\ \sigma(x,t) & \sigma(y,t) & \sigma(z,t) & 2t_3t_4 \end{pmatrix} = \nu \cdot \begin{pmatrix} B_{00} & * & * & * \\ B_{10} & B_{11} & * & * \\ B_{20} & B_{21} & B_{22} & * \\ B_{30} & B_{31} & B_{32} & B_{33} \end{pmatrix}$$

where $\sigma(a,b) = a_3b_4 + a_4b_3$.

Quadratic identities on $\mathcal{K}$

These formulas give rise to an identity [Cos11]

$$\begin{pmatrix} 2x_3x_4 & * & * & * \\ \sigma(x,y) & 2y_3y_4 & * & * \\ \sigma(x,z) & \sigma(y,z) & 2z_3z_4 & * \\ \sigma(x,t) & \sigma(y,t) & \sigma(z,t) & 2t_3t_4 \end{pmatrix} = \nu \cdot \begin{pmatrix} B_{00} & * & * & * \\ B_{10} & B_{11} & * & * \\ B_{20} & B_{21} & B_{22} & * \\ B_{30} & B_{31} & B_{32} & B_{33} \end{pmatrix}$$

where $\sigma(a,b) = a_3b_4 + a_4b_3$. Thus

$$(x_3 : y_3 : z_3 : t_3)\,, \quad (x_4 : y_4 : z_4 : t_4)$$

are the *unique* solutions to

$$\begin{aligned} B_{11} \cdot x^2 - 2 \cdot B_{10} \cdot xy + B_{00} \cdot y^2 &= 0\,, \\ B_{22} \cdot x^2 - 2 \cdot B_{20} \cdot xz + B_{00} \cdot z^2 &= 0\,, \\ B_{33} \cdot x^2 - 2 \cdot B_{30} \cdot xt + B_{00} \cdot t^2 &= 0\,, \\ B_{22} \cdot y^2 - 2 \cdot B_{21} \cdot yz + B_{11} \cdot z^2 &= 0\,, \\ B_{33} \cdot y^2 - 2 \cdot B_{31} \cdot yt + B_{11} \cdot t^2 &= 0\,, \\ B_{33} \cdot z^2 - 2 \cdot B_{32} \cdot zt + B_{22} \cdot t^2 &= 0 \end{aligned}$$

Summarizing verification on $\mathcal{K}$

Given a signature $(\mathbf{x}(R) \mid\mid s)$ on M w.r.t. $\mathbf{x}(Q)$

(1) $c \leftarrow H(\mathbf{x}(R) \mid\mid M)$

(2) $\mathbf{x}(T_0) \leftarrow \mathbf{x}([s]P)$

(3) $\mathbf{x}(T_1) \leftarrow \mathbf{x}([c]Q)$

(4) Compute all B_{IJ} for $\mathbf{x}(T_0)$ and $\mathbf{x}(T_1)$

(5) Check 6 quadratic polynomial equations in $\mathbf{x}(R)$

Efficiency of the B_{IJ}

Computing the B_{IJ} on $\mathcal{K}$ does not look great.

Efficiency of the B_{IJ}

Computing the B_{IJ} on $\mathcal{K}$ does not look great. We have

$$\begin{array}{ccccc} \text{[CC86]} & & & & \text{[Gau07]} \\ \mathcal{K} & \xrightarrow{\mathcal{H}} & \mathcal{K}^{\mathsf{Int}} & \xrightarrow{\widehat{\mathcal{C}}} & \widehat{\mathcal{K}}^{\mathsf{Gau}} \end{array}$$

Efficiency of the B_{IJ}

Computing the B_{IJ} on $\mathcal{K}$ does not look great. We have

$$\begin{array}{ccccc} \text{[CC86]} & & & & \text{[Gau07]} \\ \mathcal{K} & \xrightarrow{\mathcal{H}} & \mathcal{K}^{\mathsf{Int}} & \xrightarrow{\widehat{\mathcal{C}}} & \widehat{\mathcal{K}}^{\mathsf{Gau}} \end{array}$$

- The forms $\widehat{B}_{IJ}^{\mathsf{Gau}}$ on $\widehat{\mathcal{K}}^{\mathsf{Gau}}$ are nice, but need extra constants
- Pulling back all the way via $\mathcal{H} \circ \widehat{\mathcal{C}}$ destroys nice symmetry

Efficiency of the B_{IJ}

Computing the B_{IJ} on $\mathcal{K}$ does not look great. We have

$$\begin{array}{ccccc} \text{[CC86]} & & & & \text{[Gau07]} \\ \mathcal{K} & \xrightarrow{\mathcal{H}} & \mathcal{K}^{\mathsf{Int}} & \xrightarrow{\widehat{\mathcal{C}}} & \widehat{\mathcal{K}}^{\mathsf{Gau}} \end{array}$$

- The forms $\widehat{B}_{IJ}^{\mathsf{Gau}}$ on $\widehat{\mathcal{K}}^{\mathsf{Gau}}$ are nice, but need extra constants
- Pulling back all the way via $\mathcal{H} \circ \widehat{\mathcal{C}}$ destroys nice symmetry

Solution: Pull back $\widehat{B}_{IJ}^{\mathsf{Gau}}$ via $\widehat{\mathcal{C}}$, evaluate at $\mathcal{H}(\mathbf{x}(P))$

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}

Point compression

- Signatures $(\mathbf{x}(R) \mid\mid s)$
- Have $\mathcal{K} \subset \mathbb{P}^3$, so

$$\mathbf{x}(R) = (x : y : z : t) = (\frac{x}{t} : \frac{y}{t} : \frac{z}{t} : 1) \qquad (\text{if } t \neq 0)$$

  At first sight need 48 bytes to represent $\mathbf{x}(R)$
- Compressing further seems to require solving a *quartic*

Point compression

- Signatures $(\mathbf{x}(R) \mid\mid s)$
- Have $\mathcal{K} \subset \mathbb{P}^3$, so

$$\mathbf{x}(R) = (x : y : z : t) = (\frac{x}{t} : \frac{y}{t} : \frac{z}{t} : 1) \qquad (\text{if } t \neq 0)$$

  At first sight need 48 bytes to represent $\mathbf{x}(R)$
- Compressing further seems to require solving a *quartic*
- But have a projection $\pi : \mathcal{K} \to \mathbb{P}^2$ as a double cover

Point compression

Take the four nodes $N_0, \ldots, N_3$ and an isomorphism

$$N_0 \mapsto (0:0:0:1)\,, \qquad N_1 \mapsto (0:0:1:0)\,,$$
$$N_2 \mapsto (0:1:0:0)\,, \qquad N_3 \mapsto (1:0:0:0)\,.$$

Point compression

Take the four nodes $N_0, \ldots, N_3$ and an isomorphism

$$N_0 \mapsto (0:0:0:1)\,, \qquad N_1 \mapsto (0:0:1:0)\,,$$
$$N_2 \mapsto (0:1:0:0)\,, \qquad N_3 \mapsto (1:0:0:0)\,.$$

Then

$$\mathcal{K} : 4C \cdot xyzt = \begin{array}{c} r_1^2(xy+zt)^2 + r_2^2(xz+yt)^2 + r_3^2(xt+yz)^2 \\ -\,2r_1s_1((x^2+y^2)zt + xy(z^2+t^2)) \\ -\,2r_2s_2((x^2+z^2)yt + xz(y^2+t^2)) \\ -\,2r_3s_3((x^2+t^2)yz + xt(y^2+z^2)) \end{array}$$

Point compression

Take the four nodes $N_0, \ldots, N_3$ and an isomorphism

$$\begin{aligned} N_0 &\mapsto (0:0:0:1)\,, & N_1 &\mapsto (0:0:1:0)\,, \\ N_2 &\mapsto (0:1:0:0)\,, & N_3 &\mapsto (1:0:0:0)\,. \end{aligned}$$

Then

$$\mathcal{K} : 4C \cdot xyzt = \begin{array}{c} r_1^2(xy+zt)^2 + r_2^2(xz+yt)^2 + r_3^2(xt+yz)^2 \\ -\,2r_1s_1((x^2+y^2)zt + xy(z^2+t^2)) \\ -\,2r_2s_2((x^2+z^2)yt + xz(y^2+t^2)) \\ -\,2r_3s_3((x^2+t^2)yz + xt(y^2+z^2)) \end{array}$$

Quadratic in all its variables! Projection away from N_0 is

$$\pi : (x : y : z : t) \mapsto (x : y : z)$$

which we can represent in 32 bytes.

Point compression

Take the four nodes $N_0, \ldots, N_3$ and an isomorphism

$$N_0 \mapsto (0:0:0:1)\,, \qquad N_1 \mapsto (0:0:1:0)\,,$$
$$N_2 \mapsto (0:1:0:0)\,, \qquad N_3 \mapsto (1:0:0:0)\,.$$

Then

$$\mathcal{K} : 4C \cdot xyzt = \begin{array}{c} r_1^2(xy+zt)^2 + r_2^2(xz+yt)^2 + r_3^2(xt+yz)^2 \\ -\,2r_1s_1((x^2+y^2)zt + xy(z^2+t^2)) \\ -\,2r_2s_2((x^2+z^2)yt + xz(y^2+t^2)) \\ -\,2r_3s_3((x^2+t^2)yz + xt(y^2+z^2)) \end{array}$$

Quadratic in all its variables! Projection away from N_0 is

$$\pi : (x:y:z:t) \mapsto (x:y:z)$$

which we can represent in 32 bytes.

Recovery is solving a quadratic, *ie.* computing a square root

Implementing the scheme

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

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

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

Table: AVR ATmega comparison (rounded)

Implementing the scheme

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

Table: AVR ATmega comparison (rounded)

Thanks!

Questions?

References I

[Ber+14] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange and Peter Schwabe. "Kummer Strikes Back: New DH Speed Records". In: *Advances in Cryptology – ASIACRYPT 2014*. Ed. by Palash Sarkar and Tetsu Iwata. Vol. 8873. LNCS. https://cryptojedi.org/papers/#kummer. SV, 2014, pp. 317–337.

[CC86] David V. Chudnovsky and Gregory V. Chudnovsky. "Sequences of numbers generated by addition in formal groups and new primality and factorization tests". In: *Adv. in Appl. Math.* 7 (1986), pp. 385–434.

[Cos11] Romain Cosset. "Applications des fonctions theta à la cryptographie sur les courbes hyperelliptiques". https://tel.archives-ouvertes.fr/tel-00642951/file/main.pdf. PhD thesis. Université Henri Poincaré - Nancy I, 2011.

[Gau07] Pierrick Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *J. Mathematical Cryptology* 1.3 (2007). https://eprint.iacr.org/2005/314/, pp. 243–265.

References II

[GS12] Pierrick Gaudry and Eric Schost. "Genus 2 point counting over prime fields". In: *J. Symb. Comput.* 47.4 (2012), pp. 368–400. DOI: 10.1016/j.jsc.2011.09.003. URL: http://dx.doi.org/10.1016/j.jsc.2011.09.003.

[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.

References III

[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.

[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.