Fast explicit formulae for genus 2 hyperelliptic curves using projective coordinates

Vladyslav Kovtun
Kharkiv Air Force University
Ukraine

Thomas Wollinger
Escrypt – embedded security GmbH
Germany

4th International Conference on
Information Technology : New Generations
April 2-4, 2007, Las Vegas, Nevada, USA

Why Use Hyperelliptic Curve Cryptosystems (HECC)?

- Shorter operand length than Elliptic curve cryptosystem (ECC) $\Rightarrow$ looks promising
- Hopefully as secure as ECC
- But open questions: performance of HECC?

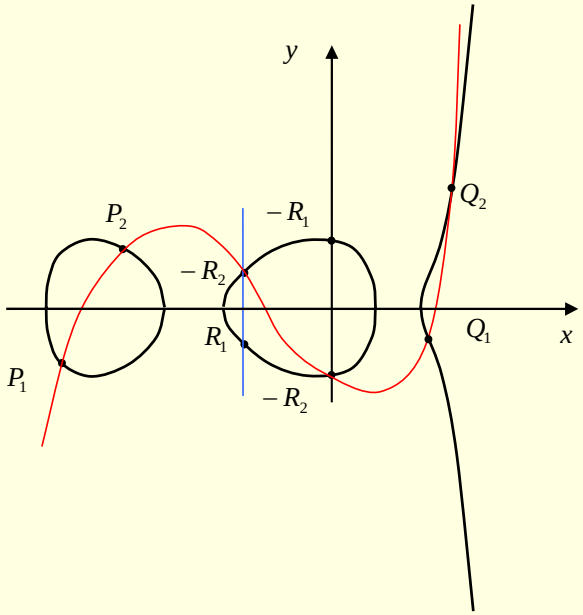
General provisions

- **Goal:** speed-up cryptosystem based on genus 2 Hyperelliptic curves
- **How:** decreasing computational complexity of public-key algorithms based on arithmetic's of Jacobian of Hyperelliptic curve
- **Target:** genus 2 Hyperelliptic curve using projective coordinates
- **Subject of investigation:** explicit formulas for divisor addition and doubling

Task

- Create method of arithmetic's in Jacobian genus 2 hyperelliptic curve with decreased computational complexity

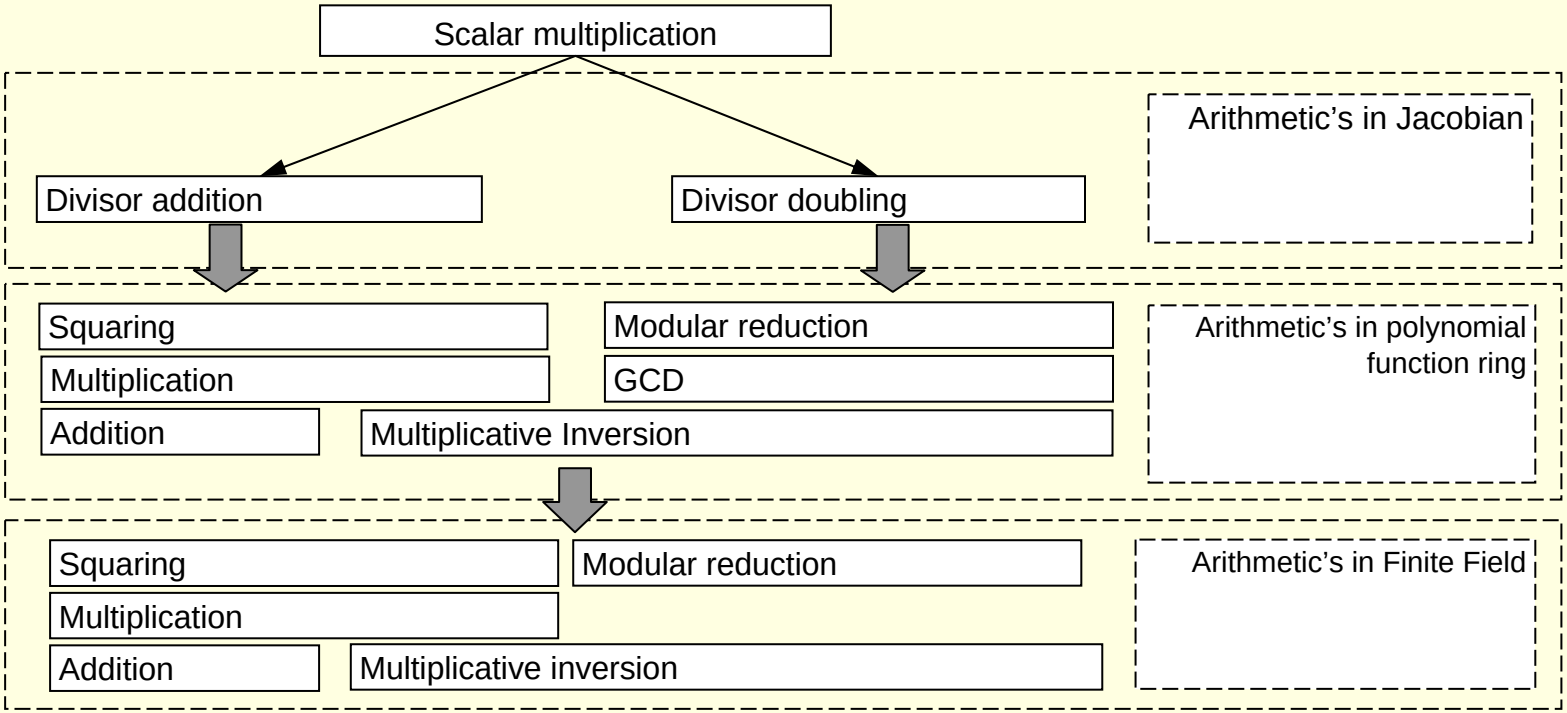
Group Arithmetic's



Picture. Geometrical interpretation of divisor addition in Jacobian of genus 2 Hyperelliptic curves

If given reduced divisors $D_1 = P_1 + P_2 - 2\infty$ and $D_2 = Q_1 + Q_2 - 2\infty$ in the Jacobian of Hyperelliptic curve genus 2, then their sum will be reduced divisor $D_3 = R_1 + R_2 - 2\infty$.

Arithmetic's hierarchy



Picture. Hierarchy of operations used in the divisor scalar multiplication

Used approaches

- Simplification of the arithmetic procedures
  $\Rightarrow$ by performing normalization
  [Lange, Wollinger]
- Normalization and minimization of Hamming weights of HEC parameters by special curves
  [Byramjee, Miyamoto & co, Lange, Stevens, Wollinger]
- Simultaneous inversion of field elements
  $\Rightarrow$ by applying the Montgomery method
  [Harley, Lange, Wollinger]
- Multiplication of polynomial functions with different powers
  $\Rightarrow$ by applying the Karatsuba method
  [Wollinger]
- Efficient modular reduction of polynomial functions
  $\Rightarrow$ by applying the Karatsuba method
  [Harley]
- Exclude inversion over field
  $\Rightarrow$ by applying the projective representation of divisors
  [Miyamoto & co, Lange, Wollinger]

Compare with previous results

Estimate computational complexity

Odd characteristic fields

Conditions	Addition			Mixed addition			Doubling		
	$()^{-1}$	^2	*	$()^{-1}$	^2	*	$()^{-1}$	^2	*
Odd characteristic field									
Affine coordinates									
$f_4 = 0$ [9]	1	3	22				1	5	22
Projective coordinates									
$\deg(h) = 2$, $h_i \in \mathbf{F}_2$ [12]		4	47		3	40		6	40
$\deg(h) = 2$, $h_i \in \mathbf{F}_2$ [proposed]		**4**	**46**		**4**	**39**		**6**	**39**

Even characteristic fields

Conditions	Addition			Mixed addition			Doubling		
	$()^{-1}$	^2	*	$()^{-1}$	^2	*	$()^{-1}$	^2	*
Even characteristic field									
Affine coordinates									
$f_4 = 0$ [6, 9]	1	3	22				1	5	22
$h_2 = 0$, $f_4 = 0$ [6, 9]	1	3	21				1	5	17
$h(x) = x$, $f_4 = 0$, $f_3 = f_2 = 0$ [6]							1	6	9
$h(x) = x$, $f(x) = x^5 + f_3 x^3 + \varepsilon x^2 + f_0$, $\varepsilon \in \mathbf{F}_2$ [14]	1		24				1	5	13
$\deg(h) = 2$, $h_0 = 0$, $h_1 \in \mathbf{F}_q$, $f(x) = x^5 + \varepsilon x^4 + f_1 x + f_0$, $\varepsilon \in \mathbf{F}_2$ [14]	1		25				1	4	22
$h_1 \in \mathbf{F}_q$, $h_2 = h_0 = 0$, $f_4 = f_1 = 0$ [15]							1	5	9
$h_1 = 1$, $h_2 = h_0 = 0$, $f_4 = f_1 = 0$ [15]							1	6	5
$\deg(h) = 2$, $h_0 = 0$, $h_1 \in \mathbf{F}_q$, $f_3 = f_2 = 0$ [15]							1	5	17
$\deg(h) = 2$, $h_0 = 0$, $h_1 \in \mathbf{F}_2$, $f_3 = f_2 = 0$ [15]							1	6	12
Projective coordinates									
$h_2 = 0$, $f_4 = 0$ [9]		4	49		4	39		7	38
$h(x) = x$, $f_4 = 0$, $f_3 = f_2 = 0$ [6]		5	45		5	38		7	31
$h(x) = x$, $f_4 = 0$, $f_3 = f_2 = 0$ [proposed]		**4**	**44**		**5**	**37**		**7**	**29**
$\deg(h) = 2$, $h_i \in \mathbf{F}_q$, $f_4 = 0$ [14]					3	42		6	39
$\deg(h) = 2$, $h_0 = 0$, $h_1 \in \mathbf{F}_q$, $f(x) = x^5 + \varepsilon x^4 + f_1 x + f_0$, $\varepsilon \in \mathbf{F}_2$ [14]						45		6	38
$h(x) = x$, $f(x) = x^5 + f_3 x^3 + \varepsilon x^2 + f_0$, $\varepsilon \in \mathbf{F}_2$ [14]					3	39		5	26

Scientific novelty of results

- Developed method of arithmetic's in Jacobian of genus 2 hyperelliptic curves in projective coordinates for the fast scalar multiplication in Jacobian of genus 2 hyperelliptic curves, what distinguished from existent by consideration earlier not known dependences between resulting divisor coordinates – polynomial functions, what allow decrease the computational complexity.
- Thus, theory of arithmetic's in Jacobian of hyperelliptic curve was further developed.

Explicit formulas

Odd characteristic fields

$v^2+h(x)v=f(x)$, $h(x)=h_2x^2+h_1x+h_0$,

$f(x)=x^5+f_4x^4+f_3x^3+f_2x^2+f_1x+f_0$, $f_4\in\mathbf{F}_2$, $f_i\in\mathbf{F}_q$

Mixed addition

Input:	$[U_{11}, U_{10}, V_{11}, V_{10}, 1], [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$	
Output:	$[U'_1, U'_0, V'_1, V'_0, Z'] = [U_{11}, U_{10}, V_{11}, V_{10}, 1] + [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$	
	Operations	Cost
1	Precomputation: $\tilde{U}_{11} = Z_2 \cdot U_{11}$, $y_1 = \tilde{U}_{11} - U_{21}$, $y_2 = U_{20} - U_{10} \cdot Z_2$.	2M
2	Computation of r for u_1 and u_2: $y_3 = U_{11} \cdot y_1 + y_2$, $r = y_2 \cdot y_3 + y_1^2 \cdot U_{10}$.	1S, 3M
3	Computation $inv = r/u_2 \bmod u_1$, $inv = inv_1 x + inv_0$: $inv_1 = y_1$, $inv_0 = y_3$.	
4	Computation of $s = (v_1 - v_2) inv \bmod u_1$, $s = s_1 x + s_0$: $w_0 = V_{10} \cdot Z_2 - V_{20}$, $w_1 = V_{11} \cdot Z_2 - V_{21}$, $w_2 = inv_0 \cdot w_0$, $w_3 = inv_1 \cdot w_1$, $s_1 = (inv_0 + inv_1) \cdot (w_0 + w_1) - w_2 - w_3 \cdot U_{11}$, $s_0 = w_2 - U_{10} \cdot w_3$. If $s_1 = 0$ then <Special case is considered>	7M
5	$R = r \cdot Z_2$, $s_2 = s_0 \cdot Z_2$, $s_3 = s_1 \cdot Z_2$, $\tilde{R} = R \cdot s_3$, $w_0 = s_1 \cdot s_0$, $w_1 = s_1 \cdot s_3$, $w_2 = s_0 \cdot s_3$, $w_3 = w_1 \cdot U_{21}$, $w_4 = R \cdot s_1$.	9M
6	Computation of $l = su_2$: $l_0 = w_0 \cdot U_{20}$, $l_2 = w_3 + w_2$, $l_1 = (w_1 + w_0) \cdot (U_{21} + U_{20}) - l_0 - w_3$.	2M
7	Computation of $u' = (s(l + h + 2v_1) - k) u_1^{-1}$, $k = (f - v_1 h - v_1^2) / u_1$: $\tilde{U}'_1 = 2w_2 - s_3 \cdot s_1 y_1 + h_2 \tilde{R} - R^2$, $\tilde{U}'_0 = s_2^2 + s_1 \cdot y_1 \cdot (s_1 \cdot \tilde{U}_{11} - 2s_2) + y_2 \cdot w_1 + 2w_4 \cdot V_{21} + h_1 \tilde{R} + R \cdot [h_2 (s_2 - s_1 \tilde{U}_{11}) + r \cdot (y_1 + 2U_{21} - f_4 Z_2)]$.	2S, 8M
8	Correction: $U'_0 = \tilde{U}'_0 \cdot \tilde{R}$, $U'_1 = \tilde{U}'_1 \cdot \tilde{R}$, $Z' = s_3^2 \cdot \tilde{R}$.	1S, 3M
9	Computation of $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v'_1 x + v'_0$: $V'_1 = \tilde{U}'_1 \cdot (l_2 - \tilde{U}'_1 + h_2 \tilde{R}) + s_3^2 \cdot (\tilde{U}'_0 - h_1 \tilde{R} - w_4 V_{21} - l_1)$, $V'_0 = \tilde{U}'_0 \cdot (l_2 - \tilde{U}'_1 + h_2 \tilde{R}) - s_3^2 \cdot (l_0 + h_0 \tilde{R} + w_4 \cdot V_{20})$.	5M
		4S, 39M

Doubling

Input:	$[U_1, U_0, V_1, V_0, Z]$	
Output:	$[U'_1, U'_0, V'_1, V'_0, Z'] = 2[U_1, U_0, V_1, V_0, Z]$	
	Operations	Cost
1	Precomputation: $Z_2 = Z^2$, $\tilde{V}_1 = h_1 Z + 2V_1 - h_2 U_1$, $\tilde{V}_0 = h_0 Z + 2V_0 - h_2 U_0$.	1S
2	Computation of r for u and $h+2v$ (while $\tilde{v} \equiv (h+2v) \bmod u$): $w_0 = V_1^2$, $w_1 = U_1^2$, $w_2 = \tilde{V}_1^2 = h_1^2 Z_2 + 4w_0 - h_2^2 w_1$, $w_3 = \tilde{V}_0 \cdot Z - U_1 \cdot \tilde{V}_1$, $r = \tilde{V}_0 \cdot w_3 + w_2 \cdot U_0$.	2S, 4M
3	Computation $inv \equiv r/\tilde{v} \bmod u$, $inv = inv_1 x + inv_0$: $inv_1 = -\tilde{V}_1$, $inv_0 = w_3$.	
4	Computation of $k \equiv \left[\left(f - hv - v^2\right)/u\right] \bmod u$, $k = k_1 x + k_0$: $w_3 = f_3 \cdot Z_2 + w_1$, $k_1 = 2w_1 + w_3 - Z \cdot (w_4 + 2 f_4 U_1 + h_2 V_1)$, $w_4 = 2U_0$, $k_0 = U_1 \cdot (Z \cdot (2w_4 + f_4 U_1 + h_2 V_1) - w_3) + Z \cdot (Z \cdot (f_2 \cdot Z - h_1 V_1 - h_2 V_0 - 2 f_4 U_0) - w_0)$.	7M
5	Computation of $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$: $w_0 = k_0 \cdot inv_0$, $w_1 = k_1 \cdot inv_1$, $s_0 = w_0 - Z \cdot U_0 \cdot w_1$, $s_3 = (inv_0 + inv_1) \cdot (k_0 + k_1) - w_0 - w_1 \cdot (1 + U_1)$, $s_1 = s_3 \cdot Z$. If $s_1 = 0$ then <Special case is considered>	7M
6	$R = r \cdot Z_2$, $\tilde{R} = R \cdot s_1$, $w_0 = s_1 \cdot s_3$, $w_1 = s_0 \cdot s_3$, $w_3 = w_1 \cdot Z$, $w_4 = R \cdot s_3$.	6M
7	Computation of $l = su$: $l_0 = U_0 \cdot w_1$, $l_2 = U_1 \cdot w_0$, $l_1 = (w_1 + w_0) \cdot (U_1 + U_0) - l_0 - l_2$.	3M
8	Computation of $u' = \left\lfloor l^2 + \frac{1}{s} l(2v+h) - \frac{1}{s^2}\left(f - vh - v^2\right) \right\rfloor / u^2$: $\tilde{U}'_1 = 2w_3 + h_2 \tilde{R} - R^2$, $\tilde{U}'_0 = s_0^2 + 2w_4 \cdot V_1 + R \cdot (h_1 s_1 + U_1 \cdot (2r \cdot Z - h_2 s_3) + h_2 s_0 - f_4 R)$.	2S, 4M
9	Correction: $U'_0 = \tilde{U}'_0 \cdot \tilde{R}$, $U'_1 = \tilde{U}'_1 \cdot \tilde{R}$, $Z' = s_1^2 \cdot \tilde{R}$.	1S, 3M
10	Computation of $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v'_1 x + v'_0$: $V'_1 = \tilde{U}'_1 \cdot (l_2 - \tilde{U}'_1 + w_3 + h_2 \tilde{R}) + s_1^2 \cdot (\tilde{U}'_1 - h_1 \tilde{R} - w_4 V_1 - l_1)$, $V'_0 = \tilde{U}'_0 \cdot (l_2 - \tilde{U}'_1 + w_3 + h_2 \tilde{R}) - s_1^2 \cdot (l_0 + h_0 \tilde{R} + w_4 \cdot V_0)$.	5M
		6S, 39M

Explicit formulas

Even characteristic fields

$v^2+h(x)v=f(x)$, $h(x)=x$, $f(x)=x^5+f_1x+f_0$, $f_i \in \mathbf{F}_2$

Mixed addition

Input:	$[U_{11}, U_{10}, V_{11}, V_{10}, 1], [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$
Output:	$[U'_1, U'_0, V'_1, V'_0, Z'] = [U_{11}, U_{10}, V_{11}, V_{10}, 1] + [U_{21}, U_{20}, V_{21}, V_{20}, Z_2]$

	Operations	Cost
1	Precomputation: $\tilde{U}_{11} = Z_2 \cdot U_{11}$, $y_1 = \tilde{U}_{11} + U_{21}$, $y_2 = U_{20} + U_{10} \cdot Z_2$.	2M
2	Computation of r for u_1 and u_2: $y_3 = y_1 \cdot U_{11} + y_2$, $r = y_2 \cdot y_3 + y_1^2 \cdot U_{10}$.	1S, 3M
3	Computation of $inv = r/u_2 \bmod u_1$, $inv = inv_1 x + inv_0$: $inv_1 = y_1$, $inv_0 = y_3$.	
4	Computation of $s = (v_1 - v_2) inv \bmod u_1$, $s = s_1 x + s_0$: $w_0 = V_{10} \cdot Z_2 + V_{20}$, $w_1 = V_{11} \cdot Z_2 + V_{21}$, $w_2 = inv_0 \cdot w_0$, $w_3 = inv_1 \cdot w_1$, $s_0 = w_2 + U_{10} \cdot w_3$, $s_1 = (inv_0 + inv_1) \cdot (w_0 + w_1) + w_2 + w_3 \cdot U_{11}$. If $s_1 = 0$ then <Special case is considered>	7M
5	$R = r \cdot Z_2$, $s_2 = s_0 \cdot Z_2$, $s_3 = s_1 \cdot Z_2$, $\tilde{R} = R \cdot s_3$, $w_0 = s_1 \cdot s_0$, $w_1 = s_1 \cdot s_3$, $w_2 = s_0 \cdot s_3$, $w_3 = w_1 \cdot U_{21}$, $w_4 = R \cdot s_1$.	9M
6	Computation of $l = su_2$: $l_0 = w_0 \cdot U_{20}$, $l_2 = w_3 + w_2$, $l_1 = (w_1 + w_0) \cdot (U_{21} + U_{20}) + l_0 + w_3$.	2M
7	Computation of $u' = (s(l + h + 2v_1) - k) u_1^{-1}$, $k = (f - v_1 h - v_1^2) / u_1$, $u' = x^2 + u'_1 x + u'_0$: $\tilde{U}'_0 = s_2^2 + s_1^2 \cdot y_1 U_{11} + y_2 \cdot w_1 + \tilde{R} + R \cdot r \cdot y_1$, $\tilde{U}'_1 = w_1 \cdot y_1 + R^2$.	3S, 5M
8	Correction: $U'_0 = \tilde{U}'_0 \cdot \tilde{R}$, $U'_1 = \tilde{U}'_1 \cdot \tilde{R}$, $Z' = s_3^2 \cdot \tilde{R}$.	1S, 3M
9	Computation of $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v'_1 x + v'_0$: $V'_1 = \tilde{U}'_1 \cdot (l_2 + \tilde{U}'_1) + s_3^2 \cdot (\tilde{U}'_0 + w_4 \cdot V_{21} + l_1)$, $V'_0 = \tilde{U}'_0 \cdot (l_2 + \tilde{U}'_1) + s_3^2 \cdot (l_0 + w_4 \cdot V_{20})$.	6M
		5S, 37M

Doubling

Input:	$[U_1, U_0, V_1, V_0, Z]$	
Output:	$[U'_1, U'_0, V'_1, V'_0, Z'] = 2[U_1, U_0, V_1, V_0, Z]$	
	Operations	Cost
1	Precomputation: $Z_2 = Z^2$, $w_0 = V_1^2$, $w_1 = U_1^2$, $w_2 = Z \cdot U_1$.	3S, 1M
2	Computation of r for u and $h+2v$ (while $\tilde{v} \equiv (h+2v) \bmod u$): $R = U_0 \cdot Z_2^2$.	1S, 1M
3	Computation of $inv \equiv r/\tilde{v} \bmod u$, $inv = inv_1 x + inv_0$: $inv_1 = Z$, $inv_0 = w_2$.	
4	Computation of $k \equiv \left[\left(f - hv - v^2\right)/u\right] \bmod u$: $k_1 = w_1$, $k_0 = U_1 \cdot w_1 + Z \cdot (Z \cdot V_1 + w_0)$.	3M
5	Computation of $s = k \cdot inv \bmod u$, $s = s_1 x + s_0$: $w_0 = k_0 \cdot inv_0$, $w_1 = k_1 \cdot Z$, $s_0 = w_0 + Z \cdot U_0 \cdot w_1$, $s_3 = (inv_0 + Z) \cdot (k_0 + k_1) + w_0 + w_1 \cdot (1 + U_1)$, $s_1 = s_3 \cdot Z$. If $s_1 = 0$ then <Special case is considered>	7M
6	$\tilde{R} = R \cdot s_1$, $w_0 = s_1 \cdot s_3$, $w_1 = s_0 \cdot s_3$, $w_3 = w_1 \cdot Z$, $w_4 = R \cdot s_3$.	5M
7	Computation of $l = su$: $l_0 = U_0 \cdot w_1$, $l_2 = U_1 \cdot w_0$, $l_1 = (w_1 + w_0) \cdot (U_1 + U_0) + l_0 + l_2$.	3M
8	Computation of $u' = \left\lfloor l^2 + \frac{1}{s} l(2v+h) - \frac{1}{s^2}\left(f - vh - v^2\right) \right\rfloor / u^2$: $\tilde{U}'_0 = s_0^2 + \tilde{R}$, $\tilde{U}'_1 = R^2$.	2S
9	Correction: $U'_0 = \tilde{U}'_0 \cdot \tilde{R}$, $U'_1 = \tilde{U}'_1 \cdot \tilde{R}$, $Z' = s_1^2 \cdot \tilde{R}$.	1S, 3M
10	Computation of $v' \equiv -(h + s_1 l + v_2) \bmod u'$, $v' = v'_1 x + v'_0$: $V'_0 = \tilde{U}'_0 \cdot \left(l_2 + \tilde{U}'_1 + w_3\right) + s_1^2 \cdot (l_0 + w_4 \cdot V_0)$, $V'_1 = \tilde{U}'_1 \cdot \left(l_2 + \tilde{U}'_1 + w_3\right) + s_1^2 \cdot \left(\tilde{U}'_0 + \tilde{R} + w_4 \cdot V_1 + l_1\right)$.	6M
		7S, 29M

Conclusions

- Best know explicit formulae today using projective coordinates
- Next step towards a efficient implementation of HECC
- Basis for efficient implementation of Public-Key cryptography
- Work in process: Further optimization

Questions?

Vladyslav Kovtun:
vladislav.kovtun@gmail.com

Thomas Wollinger:
http://www.wollinger.org
twollinger@escrypt.de

Thank you!

References

- [1] IEEE P1363-2000. Standard Specifications for Public Key Cryptography. Available at: http://www.ieee.org.
- [2] N. Koblitz Hyperelliptic cryptosystems. Journal of cryptology, No 1, 1989, pp.139-150.
- [3] A. M. Spallek, “Kurven vom geschlecht 2 und ihre anwendung in public-key-kryptosystemen”, PhD thesis, Universitat Gesamthochschule Essen, 1994.
- [4] U. Kriger, “Anwendung hyperellipischer kurven in der kryptographie”, Master’s thesis, Universitat Gesamthochschule, Essen, 2001.
- [5] R. Harley, “Fast arithmetic on genus 2 curves”, available at: http://cristal.infra.fr/~harley/hyper. 2000.

References

- [6] T. Wollinger, “Software and hardware implementation of hyperelliptic curve cryptosystems”, PhD dissertation. Bochum, Germany, May 2004.
- [7] Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, S. Tsujii, “A fast addition algorithm of genus two hyperelliptic curve”, In the 2002 Symposium on cryptography and information security – SCIS 2002, IEICE Japan, pp. 497-502, 2002. In Japanese.
- [8] M. Takahashi, “Improving Harley algorithms for Jacobians of genus 2 Hyperelliptic curves”, In Proc. of SCIS2002, IEICE Japan, 2002. In Japanese.
- [9] T. Lange, “Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae”, Cryptology ePrint Archive, report 2002/121, 2002. Available http://eprint.iacr.org.
- [10] H. Suguzaki, K. Matsuo, J. Chao, S. Tsujii, “An extension of Harley algorithm addition algorithm for hyperelliptic curves over finite fields of characteristic two”, Technical report ISEC2002-9, IEICE Japan, 2002. pp. 49-56.

References

- [11] D. Hankerson, J. Lopez Hernandez, A. Menezes, “Software implementation of elliptic curve cryptography over binary fields”, Cryptographic Hardware and Embedded Systems, CHES'2000, Springer-Verlag, LNCS 1965, 2001, pp 1-24.
- [12] T. Lange, “Inversion-free arithmetic on genus 2 hyperelliptic curves”, Cryptology ePrint Archive, report 2002/147, 2002. Available http://eprint.iacr.org.
- [13] T. Lange, “Weighted coordinates on genus 2 hyperelliptic curves”, Cryptology ePrint Archive, Report 2002/153, 2002. Available http://eprint.iacr.org.
- [14] B. Byramjee and S. Duquesne, “Classification of genus 2 curves over $\mathbf{F}_2$ and optimization of their arithmetic", Cryptology ePrint Archive, Report 2004/107, 2002. Available http://eprint.iacr.org.
- [15] T. Lange, M. Stevens, “Efficient Doubling on Genus Two Curves over Binary Fields”, Selected Areas in Cryptography, Springer-Verlag, LNCS 3357, 2004, pp. 170 – 181.