

Supersingular Elliptic Curves in Cryptography

Alfred Menezes

University of Waterloo

Elliptic Curve Cryptography (ECC)

Koblitz and Miller (1985)

Discrete log protocols using a group $\langle P \rangle$, where

- ▶ $P \in E(\mathbb{F}_q)$ is a point of (prime) order n ;
- ▶ E is an elliptic curve defined over \mathbb{F}_q .

Security is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP):

- ▶ Given the curve parameters, P and $R \in \langle P \rangle$, find the integer $l \in [0, n - 1]$ such that $R = lP$.
- ▶ Best general-purpose algorithm known for ECDLP takes \sqrt{n} steps.

Supersingular elliptic curves

An elliptic curve E defined over a field \mathbb{F}_q of characteristic p is **supersingular** if $p \mid t$, where $t = q + 1 - \#E(\mathbb{F}_q)$. If $p \nmid t$ then E is **ordinary**.

Koblitz considered the supersingular elliptic curve $E : Y^2 + Y = X^3$ over \mathbb{F}_{2^m} .

- ▶ $\#E(\mathbb{F}_{2^m}) = 2^m + 1$ if m is odd.
- ▶ Fast doubling: $2(x, y) = (x^4, y^4 + 1)$.
- ▶ (Bender & Castagnoli, 1989) $m = 61, m = 127$.
- ▶ (M & Vanstone, 1990) $m = 191, m = 251$.

Supersingular elliptic curves

Miller considered the supersingular elliptic curve $E : Y^2 = X^3 - aX$ over \mathbb{F}_p , where $p \equiv 3 \pmod{4}$.

- ▶ $\#E(\mathbb{F}_p) = p + 1$.

Kaliski (1986) considered the supersingular elliptic curve $E : Y^2 = X^3 + b$ over \mathbb{F}_p , where $p \equiv 2 \pmod{3}$.

- ▶ $\#E(\mathbb{F}_p) = p + 1$.

- ▶ Constructed pseudorandom bit generators whose security is equivalent to the ECDLP in $E(\mathbb{F}_p)$.

Weil and Tate pairing attacks (1990)

- ▶ Suppose that $\gcd(n, q) = 1$ and $n \nmid q - 1$.
- ▶ Let k be the smallest positive integer such that $n \mid q^k - 1$.
- ▶ Then $\exists Q \in E(\mathbb{F}_{q^k})$ of order n such that $Q \notin \langle P \rangle$.
- ▶ Let μ_n denote the n th roots of unity in \mathbb{F}_{q^k} .
- ▶ The Weil & Tate pairings yield a map $e : \langle P \rangle \times \langle Q \rangle \rightarrow \mu_n$ that is efficiently computable, bilinear, non-degenerate.
- ▶ The restriction $\bar{e} : \langle P \rangle \rightarrow \mu_n$ defined by $\bar{e}(R) = e(R, Q)$ is an efficiently-computable isomorphism.
- ▶ If k is small, then subexponential-time index-calculus algorithms can be used to solve the DLP in μ_n .
- ▶ The supersingular elliptic curves proposed by Koblitz, Miller and Kaliski have $k = 2$.

Ramifications

- ▶ Many cryptographers and practitioners were traumatized by the Weil and Tate pairing attacks.
- ▶ Their fears were somewhat alleviated by prohibiting supersingular curves from emerging ECC standards:
 - IEEE P1363 and ANSI X9.62 required that $k \geq 20$.
- ▶ Not everyone viewed supersingular curves as dead:
 - (M & Vanstone, 1993) $Y^2 + Y = X^3 + X + 1$ over $\mathbb{F}_{2^{239}}$ ($k = 4$).
 - (Koblitz, 1998) $Y^2 = X^3 - X + 1$ over $\mathbb{F}_{3^{97}}$ ($k = 6$) and $Y^2 = X^3 - X - 1$ over $\mathbb{F}_{3^{163}}$ ($k = 6$).
- ▶ But most experts remained skeptical about the security of both supersingular and ordinary elliptic curves.
- ▶ In May 1997, RSA Security posted [ECC Central](#) on their web site.

Claus Schnorr (1997)

“The discrete logarithm problem for elliptic curves is something that is fairly new. Very little research has been done on this problem. There is one specific result by Menezes, Okamoto and Vanstone, STOC 91. It gives a subexponential algorithm for discrete logarithms in supersingular elliptic curves. This suggests that the general problem is of a similar nature as the discrete log modulo primes p (i.e. in the multiplicative group mod p) and the problem of factoring integers. However we do not know subexponential algorithms for all elliptic curves...”

Claus Schnorr (1997)

“From what we know now, it looks as if the discrete logarithm problem for elliptic curves is somewhat harder than the discrete logarithm modulo primes p which itself looks a bit harder than factoring integers. But it is unreasonable to assume that it has straight exponential complexity.”

“A very particular case are elliptic curves in fields of powers of 2. They have been proposed since there the arithmetic is quite efficient. This particular choice seems to be risky. There are only a few fields that can be used. If the discrete logarithm problem collapses for these particular fields it nearly collapses for all elliptic curves of this type.”

Ron Rivest (1997)

“Elliptic curves show promise as an alternative basis on which to implement public-key cryptography. They are a plausible “back-up” to RSA in case should someone discover a fast integer factorization algorithm. And in some applications their apparent ability to utilize smaller public keys might be of interest.”

“But the security of cryptosystems based on elliptic curves is not well understood, due in large part to the abstruse nature of elliptic curves. Few cryptographers understand elliptic curves, so there is not the same widespread understanding and consensus concerning the security of elliptic curves that RSA enjoys....”

Ron Rivest (1997)

“...Over time, this may change, but for now trying to get an evaluation of the security of an elliptic-curve cryptosystem is a bit like trying to get an evaluation of some recently discovered Chaldean poetry. Until elliptic curves have been further studied and evaluated, I would advise against fielding any large-scale applications based on them.”

“In the end, time will tell how well they stand up to attack.”

Arjen Lenstra (1997)

“It is true that 160-bit elliptic curve cryptosystems may offer some advantages compared to 1024-bit RSA: smaller keys, less communication, storage, and faster computation. But if I would have to make a choice today between the two, purely based on perceived security, I would opt for 1024-bit RSA. The elliptic curve discrete logarithm problem has been around for a relatively short amount of time. In my opinion only relatively few people have looked at it. Therefore, we cannot yet feel sufficiently confident, where it should be noted that even marginal progress could have very damaging consequences for the security of 160-bit elliptic curve cryptosystems. Thus, right now I think it would not be prudent to switch from 1024-bit RSA to 160-bit elliptic curve cryptosystems.”

XTR

- ▶ Lenstra & Verheul (CRYPTO 2000)
- ▶ Faster than ECC and RSA.
- ▶ $n \mid p^2 - p + 1 \mid p^3 + 1 \mid p^6 - 1$, where $p \equiv 2 \pmod{3}$.
- ▶ XTR group X : order- n subgroup of $\mathbb{F}_{p^6}^*$.
- ▶ $g \in X$ is represented as $\text{Tr}_{p^6, p^2}(g)$.
- ▶ **ECSTR**: **E**fficient **C**ompact **S**ubgroup **T**race **R**epresentation
- ▶ “XTR is not affected by the uncertainty still marring ECC”
- ▶ **ECSTR**: **E**lliptic **C**urves **S**till **T**oo **R**isky

XTR and singular elliptic curves

- ▶ $X \subset S$, where S is the order- $(p^3 + 1)$ subgroup of $\mathbb{F}_{p^6}^*$.
- ▶ Suppose that $p^3 \equiv 3 \pmod{4}$, so $\mathbb{F}_{p^6} = \mathbb{F}_{p^3}(i)$, and consider $E : Y^2 = X^3 - X^2$ over \mathbb{F}_{p^3} .
- ▶ E is a singular curve with singular point $(0, 0)$.
- ▶ The map $\phi : E_{ns}(\mathbb{F}_{p^3}) \longrightarrow S$ defined by
$$\infty \mapsto 1 \quad (x, y) \mapsto \frac{y + ix}{y - ix},$$

and the map $\psi : S \longrightarrow E_{ns}(\mathbb{F}_{p^3})$ defined by

$$1 \mapsto \infty \quad u \mapsto \left(\frac{-4u}{(u-1)^2}, \frac{-4u(u+1)i}{(u-1)^3} \right)$$

are efficiently computable isomorphisms.

- ▶ **ECSTR**: **E**lliptic **C**urve **S**ingular **T**race **R**epresentation

XTR and supersingular elliptic curves

- ▶ Let $\beta \in \mathbb{F}_{p^2}$ be a square but not a cube.
- ▶ The elliptic curve $E : Y^2 = X^3 + \beta$ is supersingular and $\#E(\mathbb{F}_{p^2}) = p^2 - p + 1$.
- ▶ Let $P \in E(\mathbb{F}_{p^2})$ be a point of order n .
- ▶ $\langle P \rangle$ has embedding degree $k = 3$, and the Weil/Tate pairings give an efficiently computable isomorphism $\phi : \langle P \rangle \longrightarrow X \subset \mathbb{F}_{p^6}^*$.
- ▶ In 2000, we asked whether there is an efficiently computable isomorphism $\psi : X \longrightarrow \langle P \rangle$.
- ▶ **ECSTR**: **E**lliptic **C**urve **S**upersingular **T**race **R**epresentation

Verheul's theorem

In 2001, Verheul proved the following:

Suppose that there is an efficiently-computable homomorphism ψ from the XTR group X to the order- n subgroup $\langle P \rangle$ of $E(\mathbb{F}_{p^2})$. Then the Diffie-Hellman problems in X and $\langle P \rangle$ are efficiently solvable.

Sketch of proof:

- ▶ Suppose we are given $g, g^x, g^y \in X$.
- ▶ Let $P = \psi(g)$, $Q = D(P)$, where D is a 'distortion map'.
- ▶ Let $h = e(P, Q)$. Then

$$e(\psi(g^x), D(\psi(g^y))) = e(xP, yQ) = e(P, Q)^{xy} = h^{xy}.$$

- ▶ Thus the *weak* DH problem in X is efficiently solvable.

Consequences of Verheul's theorem

Verheul conjectured that his result can be generalized whenever a group $\mu_n \subseteq \mathbb{F}_{q^k}^*$ can be efficiently embedded in a supersingular elliptic curve $E(\mathbb{F}_q)$.

He concludes that his results:

...provide evidence that the multiplicative group of a finite field provides essentially more, and in any case not less, security than the group of points of a supersingular elliptic curve of comparable size.

Pairing-based cryptography

- ▶ Joux (2000), Sakai-Ohgishi-Kasahara (2000), Boneh-Franklin (2001)
- ▶ Main tool: Weil/Tate pairings on elliptic curves with low embedding degree.
- ▶ Permitted functionality not achievable by RSA/ECC.
- ▶ Supersingular elliptic curves:
 - Joux: ($k = 2$) $Y^2 = X^3 - aX$ over \mathbb{F}_p , $p \equiv 3 \pmod{4}$.
 - BF: ($k = 2$) $Y^2 = X^3 + b$ over \mathbb{F}_p , $p \equiv 2 \pmod{3}$.
 - BKLS & GHS ($k = 6$): $Y^2 = X^3 - X \pm 1$ over \mathbb{F}_{3^m} .
- ▶ Ordinary elliptic curves:
 - Joux: $k = 1$ ordinary elliptic curves.
 - MNT, Cocks-Pinch, BN, Freeman,

Bilinear Diffie-Hellman Problem

E : Elliptic curve defined over \mathbb{F}_q .

P : Point in $E(\mathbb{F}_q)$ of prime order n .

k : Smallest positive integer such that $n \mid q^k - 1$.

μ_n : Group of n th roots of unity in \mathbb{F}_{q^k} .

Q : Order n -point in $E(\mathbb{F}_{q^k})$ such that $Q \notin \langle P \rangle$.

$e : \langle P \rangle \times \langle Q \rangle \rightarrow \mu_n$: bilinear, non-degenerate map

- ▶ **BDHP**: Given P, rP, sP and Q , compute $e(P, Q)^{rs}$.
- ▶ This is a new problem!
- ▶ The embedding degree k must be small.
- ▶ Necessary conditions for the hardness of BDHP:
 - Hardness of DHP (and DLP) in $\langle P \rangle$.
 - Hardness of DHP (and DLP) in μ_n .

Hardness of DLP in $\langle P \rangle$

- ▶ Recall that there is an efficiently-computable homomorphism from $\langle P \rangle$ to μ_n .
 - This gives an efficient reduction from DLP in $\langle P \rangle$ to the DLP in μ_n .
- ▶ Question: Is there an efficient reduction of DLP in μ_n to the DLP in $\langle P \rangle$?
- ▶ In particular, is there an efficiently-computable homomorphism from μ_n to $\langle P \rangle$?

Verheul's theorem revisited

- ▶ Let \mathbb{F}_q be an arbitrary finite field of odd characteristic. (A similar argument applies to even characteristic fields.)
- ▶ Suppose that we can efficiently construct an elliptic curve E over \mathbb{F}_q with $\#E(\mathbb{F}_q) = q + 1$.
- ▶ Then $\#E(\mathbb{F}_{q^2}) = q^2 + 1 + 2q$.
- ▶ Let \tilde{E} denote the twist of E over \mathbb{F}_{q^2} . Then $\#\tilde{E}(\mathbb{F}_{q^2}) = q^2 + 1 - 2q$ and $\tilde{E}(\mathbb{F}_{q^2}) = \mathbb{Z}_{q-1} \oplus \mathbb{Z}_{q-1}$.
- ▶ Suppose we can construct distortion maps for $\tilde{E}(\mathbb{F}_{q^2})$.
- ▶ If a Verheul homomorphism can be constructed for these curves, then the Diffie-Hellman problem is easy for *all* finite fields.

Verheul's theorem revisited

If Verheul homomorphisms can be constructed for these curves, then all pairing-based cryptosystems (and many XTR protocols) would be completely insecure.

- ▶ (Sato) Partial results on the difficulty of constructing a Verheul homomorphism (using univariate polynomial functions).
- ▶ The construction of Verheul homomorphism has no effect on the security of standard elliptic curve cryptography (using elliptic curves with very high embedding degrees).

Verheul's theorem revisited

If Verheul homomorphisms cannot be constructed, then we may not be able to prove the equivalence of the DLP and DHP in $\langle P \rangle$ and μ_n (for supersingular elliptic curves).

- ▶ This is somewhat analogous to a similar concern with RSA.
- ▶ In 1998 Boneh and Venkatesan proved that an “algebraic” reduction from factoring to the RSA problem with small encryption exponent is not possible unless both problems are easy.

Acceptance of pairing-based cryptography

It is surprising that despite the prevailing mistrust of ECC in general, and supersingular elliptic curves in particular, pairing-based cryptography (PBC) was immediately accepted by the research community.

There are three reasons for this:

1. PBC was not viewed by commercial organizations as disruptive to their interests.
2. PBC was not viewed by academic researchers as disruptive to their interests.
3. PBC protocols were presented with elaborate security proofs.

Hardness of DLP in μ_n

- ▶ Work by Granger and Vercauteren (2005) demonstrated the special nature of some groups μ_n that correspond to elliptic curves with low embedding degree.
- ▶ Index-calculus algorithms are faster than Pollard's rho method in the *full* torus $T_2(\mathbb{F}_{q^m})$ and $T_6(\mathbb{F}_{q^m})$ for $m \geq 3$.
 - $T_2(\mathbb{F}_q)$: order- $(q + 1)$ -subgroup of \mathbb{F}_{q^2} .
 - $T_6(\mathbb{F}_q)$: order- $(q^2 - q + 1)$ -subgroup of \mathbb{F}_{q^6} .
- ▶ In some special cases, index-calculus algorithms are faster than Pollard's rho method in prime order subgroups of $T_2(\mathbb{F}_{q^m})$ and $T_6(\mathbb{F}_{q^m})$.
 - Example: A 160-bit subgroup of $T_6(\mathbb{F}_{q^m})$ where $q^m = p^5$ and $p \approx 2^{33}$.

Why use supersingular curves?

- ▶ No weaknesses are known for (carefully selected) supersingular curves.
- ▶ IETF draft standard. Identity-based cryptography standard (IBCS) #1: Supersingular curve implementations of the BF and BB1 IBEs.
- ▶ Asymmetric pairings $\hat{e} : G_1 \times G_2 \longrightarrow G_T$ arising from ordinary curves do not have fast hashing to G_2 *and* an efficiently-computable isomorphism $\Psi : G_2 \longrightarrow G_1$.
- ▶ Possible applicability of the special NFS for the DLP in $\mathbb{F}_{p^{12}}$ for BN ordinary curves (preliminary work by Schirokauer, ECC 2006).
- ▶ Speed?

Speed comparisons of supersingular curves

128-bit security level

(Ahmadi, Hankerson, M.)

Pairing Type	k	\mathbb{F}_q	Curve equation	$\ n\ _2$	$\ q^k\ _2$
I	2	1536-bit p	$Y^2 = X^3 - 3X$	256	3072
II	4	$\mathbb{F}_{2^{1223}}$	$Y^2 + Y = X^3 + X$	1221	4892
III	6	$\mathbb{F}_{3^{509}}$	$Y^2 = X^3 - X + 1$	804	4841
IV	12	$\mathbb{F}_{2^{439}}$	$Y^2 + Y = X^5 + X^3$	875	5268

Type I pairing: BKLS/GHS

Type II, III, IV pairing: BGOS

Cost of curve/field operations

Cost (number of \mathbb{F}_q -mults) of the Tate pairing, point mult rP in $E(\mathbb{F}_q)$, and exponentiation α^r in μ_n .

Type	q	Tate pairing	rP, P unknown	rP, P fixed	Exp in μ_n α unknown	Exp in μ_n α fixed
I	p^{1536}	6912/4096	2602	745	512	199
II	2^{1223}	4284	1895/447	1832/384	1895/447	1832/384
III	3^{509}	3825	1259/498	1016/324	2518/996	2032/648
IV	2^{439}	15111	5043/1944	4392/1293	8262/2700	7884/2322

full-length/256-bit multiplier r

Experimental

II		4578	2163		2037	
III		4359	1602		2695	

Arithmetic in \mathbb{F}_{3^m}

- ▶ $a \in \mathbb{F}_{3^m}$ is a polynomial $a_{m-1}x^{m-1} + \dots + a_0$ for $a_i \in \mathbb{F}_3$.
- ▶ Multiplication is modulo an irreducible polynomial f of degree m .
- ▶ a_i is represented in $\{0, 1, -1\}$ using pair (a_i^0, a_i^1) of bits.

▶ **Addition** is

$$t \leftarrow (a^0 \vee b^1) \oplus (a^1 \vee b^0), \quad c^0 \leftarrow (a^1 \vee b^1) \oplus t, \quad c^1 \leftarrow (a^0 \vee b^0) \oplus t$$

▶ **Multiplication**: Karatsuba used in earlier reports.

However the comb method seems faster:

- Idea: for $c = a \cdot b$, choose $w > 0$ and compute $x^i b$ for $i < w$. Coeffs of a placed in a matrix and columns processed w at a time (index to $x^i b$).
- Multiplication times are factor 4 faster than Karatsuba method in [GPS] for $\mathbb{F}_{3^{239}}$.

Boneh-Franklin IBE

$P \in E(\mathbb{F}_q)$ is a point of order n , and $\hat{e} : \langle P \rangle \times \langle P \rangle \rightarrow \mu_n$ is a (symmetric) bilinear pairing. $H_{[1-5]}$ denote hash functions.

- ▶ TTP has private key $t \in_R [1, n - 1]$ and public key $T = tP$.
- ▶ Party A 's private key is $d = tQ$, where $Q = H_1(\text{ID}_A)$.
- ▶ To **encrypt** $m \in \{0, 1\}^\lambda$ for A , party B does:
 1. Select $\sigma \in_R \{0, 1\}^\lambda$, and compute $Q = H_1(\text{ID}_A)$,
 $r = H_2(\sigma, m)$, $R = rP$, $V = \sigma \oplus H_3(\hat{e}(T, Q)^r)$, and
 $c = m \oplus H_4(\sigma)$.
 2. B sends (R, V, c) to A .
- ▶ To **decrypt**, A computes $\sigma = V \oplus H_3(\hat{e}(d, R))$, $m = c \oplus H_4(\sigma)$,
and $r = H_2(\sigma, m)$. A accepts m if $R = rP$.

Boneh-Franklin IBE (Type IV pairing)

T, Q are degenerate divisors $[(P_1) - (\infty)]$

R, P, d are non-degenerate divisors $[(P_1) + (P_2) - 2(\infty)]$

- ▶ TTP has private key $t \in_R [1, n - 1]$ and public key $T = tP$.
- ▶ Party A 's private key is $d = tQ$, where $Q = H_1(\text{ID}_A)$.
- ▶ To **encrypt** $m \in \{0, 1\}^\lambda$ for A , party B does:
 1. Select $\sigma \in_R \{0, 1\}^\lambda$, and compute $Q = H_1(\text{ID}_A)$,
 $r = H_2(\sigma, m)$, $R = rP$, $V = \sigma \oplus H_3(\hat{e}(T, Q)^r)$, and
 $c = m \oplus H_4(\sigma)$.
 2. B sends (R, V, c) to A .
- ▶ To **decrypt**, A computes $\sigma = V \oplus H_3(\hat{e}(d, R))$, $m = c \oplus H_4(\sigma)$,
and $r = H_2(\sigma, m)$. A accepts m if $R = rP$.

Encryption/Decryption costs in \mathbb{F}_p mults

Costs normalized to \mathbb{F}_p -mults (1536-bit p) using our timings for mult of $26.5\mu\text{s}$ in \mathbb{F}_p , $15.6\mu\text{s}$ in $\mathbb{F}_{2^{1223}}$, $12.8\mu\text{s}$ in $\mathbb{F}_{3^{509}}$, and $3.0\mu\text{s}$ in $\mathbb{F}_{2^{439}}$.

	no precomp for Tate, full-length r				precomp for Tate, 256-bit r			
	I	II	III	IV	I	II	III	IV
BF encrypt	9975	4679	2829	3143	7159	2974	2161	2158
BF decrypt	7657	3600	2338	6485	4841	2748	2004	6129

Timings on a 2.4 GHz Pentium 4 running Linux/x86.

\mathbb{F}_p timings obtained using MIRACL.

No special registers were used.

Sakai-Kasahara IBE

- ▶ TTP has private key $t \in_R [1, n - 1]$ and public key $T = tP$.
- ▶ Party A 's private key is $d = (1/(H_5(\text{ID}_A) + t)P$.
- ▶ To **encrypt** $m \in \{0, 1\}^\lambda$ for A , party B does:
 1. Select $\sigma \in_R \{0, 1\}^\lambda$, and compute $Q = H_5(\text{ID}_A)P + T$, $r = H_2(\sigma, m)$, $R = rQ$, $V = \sigma \oplus H_3(\hat{e}(P, P)^r)$, and $c = m \oplus H_4(\sigma)$.
 2. B sends (R, V, c) to A .
- ▶ To **decrypt**, A computes $\sigma = V \oplus H_3(\hat{e}(d, R))$, $m = c \oplus H_4(\sigma)$, and $r = H_2(\sigma, m)$. A accepts m if $R = rQ$.

Encryption/Decryption costs in \mathbb{F}_p mults

Costs normalized to \mathbb{F}_p -mults (1536-bit p) using our timings for mult of $26.5\mu\text{s}$ in \mathbb{F}_p , $15.6\mu\text{s}$ in $\mathbb{F}_{2^{1223}}$, $12.8\mu\text{s}$ in $\mathbb{F}_{3^{509}}$, and $3.0\mu\text{s}$ in $\mathbb{F}_{2^{439}}$.

	no precomp for Tate, full-length r				precomp for Tate, 256-bit r			
	I	II	III	IV	I	II	III	IV
BF encrypt	9975	4679	2829	3143	7159	2974	2161	2158
BF decrypt	7657	3600	2338	6485	4841	2748	2004	6129
SK encrypt	3546	3272	2080	1961	3546	715	710	625
SK decrypt	7657	3600	2338	6485	4841	2748	2004	6129

Timings on a 2.4 GHz Pentium 4 running Linux/x86.

\mathbb{F}_p timings obtained using MIRACL.

No special registers were used.

Comparing Type III and BN pairings

Very rough calculations:

- ▶ Devegili-Scott-Dahab implementation of the Ate pairing for BN curves: 39.3 ms on a 3.4 GHz Pentium 4 (with SSE2 registers).
- ▶ Our implementation of the BGOS pairing for Type III curves: 55.8 ms on a 2.4 GHz Pentium 4 (without SSE2 registers), which 'scales' to 39.4 ms on a 3.4 GHz Pentium 4.

Conclusions

- ▶ Supersingular elliptic curves are very attractive for PBC.
- ▶ Don't discount the $k = 6$ supersingular elliptic curves over \mathbb{F}_{3^m} .