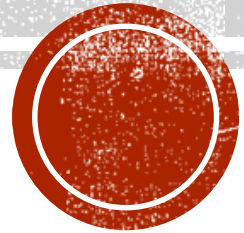
ALGORITHM FOR SHORT MESSAGES ENCRYPTION ON TWISTED EDWARD CURVES

A. BESSALOV, L. KOVALCHUK, N. KUCHYNSKA, O. TELIZHENKO

IPT National Technical University of Ukraine

“Igor Sikorsky Kyiv Polytechnic Institute”



RELATED STANDARDS

- ISO/IEC 18033-2:2006 (harmonized in Ukraine as DSTU ISO/IEC 18033-2: 2015)

  Information technology — Security techniques — Encryption algorithms

  — Part 2: Asymmetric ciphers

- Belorussian standard STB 34.101.45-2013

  Information technology and security.

  Digital signature and key transport algorithms based on elliptic curves

OUR PURPOSE

To create standard for short messages encryption with:

- Well defined procedures
- Sufficient level of security
- High performance
- With references on correspondent Ukrainian national standards

WHY EDWARDS CURVES?

- The absence of "the point on infinity"
- The fastest addition of points
- Universality of the addition law

- Why don`t we use complete Edwards curves? Symmetry: one point defines 7 other

BASIC ALGEBRAIC STRUCTURES

A finite field F_p, $p \equiv 5 \bmod 8$, with bit length $l(p)$ = 256, 384, 512, 768.

We define Edwards curve $Edw(F_p)$ over F_p:

$$Edw(F_p): x^2 + ay^2 = 1 + dx^2y^2, a \neq d, a, d \notin Q_p. \quad (1)$$

Recommended $a = 2$.

$\#Edw(F_p) = 4n$, n is prime.

DESIGNATIONS

- Security level λ, determines choice of other parameters.

  Prime number p *with bit length* $l(p) = \lfloor \log_2 p \rfloor + 1 = 2(\lambda + 1)$, *determines the finite field* F_p.
- Base point P such that $ord(P) = n$ of the curve $Edw\left(F_p\right)$.
- A private key $e \in F_p$ and the corresponding public key $Q = eP$.
- Hash-function H and its id ($iH = (0, i_6, ..., i_0)$), the length of hash-function output is l_H, *recommended to use DSTU 7564:2014 (Kupyna).*
- l-bit block and k-bit key κ of block cypher with encryption $E_{l,k}^{(\kappa)}$ and decryption $D_{l,k}^{(\kappa)}$ transformations *recommended to use DSTU 7426:2014 (Kalyna).*

ENCRYPTION

Let M be a message.

1. Choose a random integer $\varepsilon : 1 < \varepsilon < n - 1$.
2. Compute the point $R = \varepsilon P = (x_R, y_R)$, set r as a bit representation of x_R of the length $l(p)$.
3. Compute the point $T = \varepsilon Q = (x_T, y_T)$ and set $\kappa = x_T^{(k)}$ - the lowest k bit of x_T.
4. Compute $t = E_{l,k}^{(\kappa)}(M)$.
5. The ciphertext is $C = (r \| t)$.

DECRYPTION

Let $C = (r \,||\, t)$ be a cyphertext.

1. Compute $u = \left(1 - r^2\right)\left(a - dr^2\right)^{-1} \bmod p$ and root $y = \sqrt{u} \bmod p$, set $R' = \left(r, y\right)$.
2. Compute $T' = \left(x_T', y_T'\right) = eR'$ and set $x_T^{(k)}$ - the lowest k bit of x_T.
3. Compute the message $M = D_{l,k}^{(\kappa)}\left(t\right)$.

SECURITY ASPECTS

- To recover key or plaintext isn`t easier than to solve CDH or DLP.

- Encryption algorithm is CPA-secure and CCA-secure,

  if the encryption $E_{l,k}^{(\kappa)}$ is CPA and CCA-secure.

RECOMENDED PARAMETERS (λ=127)

p	1157920892373161954235709850086879078532699846656405640394575840079131296395501	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE4D
n	2894802230932904885589274625217197696337316993117180182488949587991265517486 3	400000000000000000000000000000029E26087789BC2815BDFF97093543CCF
d	24	18
x_P	6601968239031997106746018989618928059894553871212359007010535654759166748473 5	91F5D0E7E2D417E3108B13B075CDC7756045F8424479FCFE8F23D27250A0883F
y_P	5255160579431603195550695325517854265423042892790261317629215741016825673348 3	742F27A268641C9D7DDF69892BE3DF3D8F9CC52260B89A4953C8379C7C0A212B

RECOMENDED PARAMETERS (λ=191)

p	394020061963944792122790401001436138050797392704654466679482934042457217714972106114142662548849156408066279903 04669	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF79D
n	985050154909861980306976002503590345126993481761636166698734240194831149331612477994593809865442793064701305978 4399	400000000000000000000000000000000000000000000000000000AF905B73674AC7D4AF38C53331DC208A517DCB3F340EECF
d	532	214
x_P	378605099923611775822585344176526745571001455847209534083111347984587035202012457786807657785870884173242153300 90097	F5FC151B6264CB53A4B879AA9A1F4A5156BBF063B56AAA912617C0E4CEFF15D2DF497D9AEF12374A22D22C3B402B2C71
y_P	260129509132952349786225203482071189933725997538504879752092777989029134090282419473324707561401813312992987967 92753	A9027207E88074F4AFA3D44D4590DD04BAFBF6AE3D321091F500C783F4707940B7F5EBDD93325C5391843F9A78526BB1

RECOMENDED PARAMETERS (λ=255)

p	134078079299425970995740249982058461274793658 2 0592393377723561443721764030073546976801874298 1669034276900318581864860508537538828119465699 46433649006083221	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFC95
n	3351951982485649274893506249551461531869841455 1480983444308903609304410075184051261344573622 0066515147934100158598747475094307363660134140 2240469528982943	4000000000000000000000000000000000000000000 00000000000000000000028A3CE52209E2BD49528 82D5574165192C46C0D0311FEA6BF9FECE70EE6 3B59F
d	269	10D
x_P	4304638059767723691843448011416912131787206520 4166094567972647848418035311036617847132303732 2943652452004529525462264461822135736467276791 4084560567247872	5230A1EE747050A072BD7319741586EA520388B6 B53094571C821A2FC9A9E83D56665346B5DB04C 43E75261DBDA512728FAAFAC48AE9260A5A18 4E2933E3A400
y_P	2737479309967709176042361051055657634308979151 4222859156372319061778945606835359017625712614 1281310823616344249693945914310794442807188517 297401383160453	53A0D50CC63C9219762F451978AEF214DBCFCC 3A5CB5EF27124991A86B42B3A1A832724A0E6B 930FDD1DA2E27A540D6B675E4422C444F529C5 08F0BAE7D0A85

RECOMENDED PARAMETERS (λ=383)

p	155251809230070893514897948846250255525688601711669661113905203802605095268637688633087840882864647795048773069713107320617158004411481439144428727504118113920445497602084990555026528563159844482526299919371646875089284685381604 8197	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDA45
n	388129523075177233787244872115625638814221504279174152784763009506512738171594221582719602207161619487621932674282778802681788026146710554564634213074757226667387371018921502655542196864868529764392314827466782773958794286583799363	4000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000443A2EC4A0EE2AA34439FF2239B2E0A486E21A23CCBF0266B649F83B9C234F6A0FF7785DACE4C8F581D4D96C68345E43
d	604	25C
x_P	741459216301541774273999570424768582365165501397353071412416913875335429430795815824885238553733362236849221592468135073419283135668359442111349679479307093480514005002056875106774949056454938706352135933708099821096151656645902040	7A4301399505745D99DC7F4FC4E931300E4DC193DF1E7BA1B579ABDE4D2E32BEBFB593B148406544D16D5585DF369A7AF65C2D6258F48FC8C5D0E42D51EBE8B250B3B1DAB47FC3698FCAAA86C62CCFE83E887850D0995A58D41471AB9285BED8
y_P	863069083887035270377922930301493822620184485473894448032477577527897743811058624597730587709630551511602940926595014026271147153351515528318763965711144202510924166157941979659056904718817367848932767618504909932832278276957883683	8E507CB7494E04A4624223110A0FDBD63CDC40376E4786FF960B8D39B25E949C96EA40BBC4A59CB9DD902CCFFEE583BAA7D0FCE6E0D9F75742B08A13E29068E39DCE12816E52FA1411D89C76476012C979D93A863268D0D096CC98EE9A894D23

THANK YOU FOR ATTENTION

n.kuchynska@kpi.ua

lusi.kovalchuk@gmail.com