

# ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Únor 2012**

## **Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 5: Generování eliptických křivek**

**ČSN**  
**ISO/IEC 15946-5**  
36 9794

Information technology - Security techniques - Cryptographic techniques based on elliptic curves -  
Part 5: Elliptic curve generation

Technologies de l'information - Techniques de sécurité - Techniques cryptographiques fondées sur les  
courbes elliptiques -  
Partie 5: Génération de courbes elliptiques

Tato norma je českou verzí mezinárodní normy ISO/IEC 15946-5:2009. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 15946-5:2009. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 15946-1 dosud nezavedena

Souvisící ČSN

ČSN ISO/IEC 10118-1:2002 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně

ČSN ISO/IEC 10118-3:2004 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 3: Dedikované hašovací funkce

ČSN ISO/IEC 10118-4:2001 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

## MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 15946-5  
Kryptografické techniky založené na eliptických křivkách – První vydání  
Část 5: Generování eliptických křivek 2009-12-15

ICS 35.040

Obsah

Strana

Předmluva 5

Úvod 6

**1** Předmět normy 7

**2** Citované normativní dokumenty 7

**3** Termíny a definice 7

**4** Způsob zápisu a konverzní funkce 8

**4.1** Způsob zápisu 8

**4.2** Konverzní funkce 8

**5** Rámec pro generování eliptických křivek 9

**5.1** Typy důvěryhodných eliptických křivek 9

**5.2** Přehled generování eliptických křivek 9

**6** Generování ověřitelně pseudo-náhodné eliptické křivky 9

**6.1** Konstruování ověřitelně pseudo-náhodných eliptických křivek (případ prvočísla) 9

**6.1.1** Algoritmus konstrukce 9

**6.1.2** Test na blízkou prvočíselnost 10

**6.1.3** Nalezení řádu bodu velkého prvočísla 11

**6.1.4** Ověření pseudonáhodnosti eliptické křivky 11

**6.2** Konstruování ověřitelně pseudo-náhodných eliptických křivek (případ mocniny dvou) 12

**6.2.1** Algoritmus konstrukce 12

## 6.2.2 Ověření pseudonáhodnosti eliptických křivek 13

## 7 Konstruování eliptických křivek složenou multiplikací 13

### 7.1 Všeobecná konstrukce (případ prvočísla) 13

### 7.2 Křivka MNT (Křivka Miyaji-Nakabayashi-Takano) 14

### 7.3 Křivka BN (Křivka Barreto-Naehriga) 15

### 7.4 Křivka F (Freemanova křivka) 16

### 7.5 Křivka CP (Cocks-Pinchova křivka) 17

## 8 Konstruování eliptických křivek zvednutím 17

## Příloha A (informativní) Základní informace o eliptických křivkách 19

## Příloha B (informativní) Základní informace o kryptosystémech eliptických křivek 21

## Příloha C (informativní) Číselné příklady 23

## Příloha D (informativní) Přehled vlastností eliptických křivek generovaných metodou složené multiplikace 30

## Bibliografie 31

### Odmítnutí odpovědnosti za manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, pokud nejsou typy písma, které jsou vloženy, používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, na jejichž základě byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, že vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



### DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2009

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail [copyright@iso.org](mailto:copyright@iso.org)

Web [www.iso.org](http://www.iso.org)

Published in Switzerland

## Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří

specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnice ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících členů.

Je třeba upozornit na skutečnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nepřijímají odpovědnost za identifikaci některých nebo všech takovýchto patentových práv.

Mezinárodní norma ISO/IEC 15946-5 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie, subkomise SC 27, Bezpečnostní techniky IT.*

ISO/IEC 15946 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní techniky – Kryptografické techniky založené na eliptických křivkách*:

- Část 1: Všeobecně
- Část 5: Generování eliptických křivek

## Úvod

Mezi některé z nejzajímavějších alternativ k systémům založeným na RSA a  $F(p)$  patří kryptosystémy založené na eliptických křivkách definovaných nad konečnými poli. Pojetí kryptosystému s veřejným klíčem, který je založen na eliptických křivkách, je poměrně jednoduché:

- Každá eliptická křivka nad konečným polem je vybavena operací sčítání „+“, na základě, které vytváří konečnou Abelovskou grupu.
- Pravidlo grupy na eliptických křivkách se rozšiřuje přirozeným způsobem na „diskrétní umocňování“ na bodovou grupu eliptické křivky.
- Na základě diskrétního umocňování eliptické křivky je snadné odvodit analogie eliptické křivky známých schémat s veřejnými klíči typu Diffie-Hellmana a ElGamala.

Bezpečnost systému s veřejnými klíči závisí na obtížnosti určování diskrétních logaritmů v grupě bodů eliptické křivky. Tento problém je – na úrovni současných znalostí – mnohem těžší než faktorizace celých čísel nebo výpočet diskrétních logaritmů v konečném poli. Skutečně, od té doby, co Miller a Koblitz v roce 1985 nezávisle navrhli použití eliptických křivek pro kryptografické systémy s veřejným klíčem, problém diskrétních logaritmů eliptických křivek se ukázal řešitelný pouze v určitých specifických a snadno rozpoznatelných případech. Nedošlo k podstatnému pokroku ve hledání efektivní metody pro řešení problému diskrétních logaritmů eliptických křivek pro libovolné eliptické křivky. Je proto možné použít u systémů s veřejnými klíči založených na eliptických křivkách mnohem kratší parametry než systém RSA nebo systémy založené na klasických diskrétních logaritmech, které využívají multiplikativní grupu konečného pole. Výsledkem jsou významně kratší digitální podpisy a parametry systému.

Tato část ISO/IEC 15946 popisuje techniky generování eliptických křivek užitečné pro implementování mechanismů založených na eliptických křivkách definovaných v ISO/IEC 9796-3, ISO/IEC 11770-3,

ISO/IEC 14888-3 a ISO/IEC 18033-2.

Účelem této části ISO/IEC 15946 je vyhovět rostoucímu zájmu o technologie s veřejnými klíči založené na eliptických křivkách popisem metod generování eliptických křivek pro podporu výměny klíčů, transportu klíčů a digitálních podpisů založených na eliptických křivkách.

## 1 Předmět normy

ISO/IEC 15946 specifikuje kryptografické techniky s veřejným klíčem založené na eliptických křivkách.

Tato část ISO/IEC 15946 definuje techniky generování eliptických křivek užitečné pro implementování mechanismů založených na eliptických křivkách definovaných v ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3 a ISO/IEC 18033-2.

Předmět této části ISO/IEC 15946 je omezen na kryptografické techniky založené na eliptických křivkách definovaných nad konečnými poli řádu prvočíselné mocniny (včetně speciálních případů prvočíselného řádu a charakteristiky dvě). Zobrazení prvků základního konečného pole (tj. podle použité báze) není předmětem této části ISO/IEC 15946.

ISO/IEC 15946 nspecifikuje implementaci definovaných technik. Není zaručena interoperabilita produktů odpovídajících ISO/IEC 15946.

Konec náhledu - text dále pokračuje v placené verzi ČSN.