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

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

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

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

Web 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 Směrnic 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 nepřejímají 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 nespecifikuje implementaci definovaných technik. Není zaručena interoperabilita produktů odpovídajících ISO/IEC 15946.