ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Leden

2005

	Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 1: Všeobecně	ČSN ISO/IEC 15946-1 36 9794

Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General

Technologies de l’information - Techniques de sécurité - Techniques cyrptographiques basées sur les courbes
elliptiques - Partie 1: Généralités

Informationstechnik - IT-Sicherheitsverfahren - Kryptographische Techniken auf Basis von eliptischen Kurven -
Teil 1: Allgemeines Modell

Tato norma je českou verzí mezinárodní normy ISO/IEC 15946-1:2002. Mezinárodní norma ISO/IEC 15946-1:2002 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 15946-1:2002. The International
Standard ISO/IEC 15946 -1:2002 has the status of a Czech Standard.

71863

Národní předmluva

Citované normy

ISO/IEC 9796 (všechny části) zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Digitální podpisy umožňující obnovu zprávy

ISO/IEC 9797 (všechny části) zavedena v ČSN ISO/IEC 9797 (36 9782) Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC)

ISO/IEC 10118 (všechny části) zavedena v ČSN ISO/IEC 10118 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce

ISO/IEC 11770-3:1999 zavedena v ČSN ISO/IEC 11770-3 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 14888 (všechny části) zavedena v ČSN ISO/IEC 14888 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem

ISO/IEC 15946-2:2002 dosud nezavedena

ISO/IEC 15946-3:2002 dosud nezavedena

ISO/IEC 15946-4:2004 dosud nezavedena

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 1: Všeobecně	ISO/IEC 15946-1 První vydání 2002-12

Obsah

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 příslušnou 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 JTC1.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 3 Direktiv ISO/IEC.

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

ISO/IEC 15946-1 byla připravena společnou technickou komisí ISO/IEC JTC1, *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 2: Digitální podpisy*

– *Část 3: Ustavení klíčů*

– *Část 4: Digitální podpisy umožňující obnovu zprávy*

Přílohy A a B této části mezinárodní normy ISO/IEC 15946 mají pouze informativní charakter.

Úvod

Jednou z nejzajímavějších alternativ k systémům založeným na RSA a GF(p), které jsou v současné době dostupné, jsou kryptografické systémy založené na eliptických křivkách definovaných nad konečnými poli. Koncept kryptografického systému s veřejným klíčem založeného na eliptické křivce je poměrně jednoduchý:

– Každá eliptická křivka má binární operaci „+“, pomocí které vytváří konečnou abelovskou grupu.

– Zákon grupy se u eliptických křivek rozšiřuje přirozeným způsobem k „diskrétní exponenciaci“ bodové grupy eliptické křivky.

– Na základě diskrétní exponenciace eliptické křivky je možné snadno odvodit obdoby eliptické křivky z dobře známých schémat s veřejným klíčem Diffie-Hellmana a El Gamala.

Bezpečnost takového systému s veřejným klíčem závisí na obtížnosti určení diskrétních logaritmů v grupě bodů eliptické křivky. Tento problém je - při současné úrovni znalostí - mnohem obtížnější než faktorizace celých čísel nebo výpočet diskrétních logaritmů v konečném poli. Ve skutečnosti od té doby, co Miller a Koblitz v r. 1985 nezávisle navrhli použití eliptických křivek u kryptografických systémů s veřejným klíčem, nebyl zaznamenán žádný významný pokrok ve vypořádání se s problémem diskrétního logaritmu eliptických křivek. Obecně platí, že určit diskrétní logaritmy eliptických křivek jsou schopné pouze algoritmy, které vyžadují exponenciální čas. Je proto možné u systémů s veřejným klíčem založených na eliptických křivkách použít daleko kratší parametry než je tomu u systému RSA nebo klasických systémů založených na diskrétních logaritmech, které využívají multiplikativní grupu některého konečného pole. To přináší významně kratší digitální podpisy a systémové parametry a vyhýbá se použití výpočtů s mimořádně velkými celými čísly.

Tato část ISO/IEC 15946 popisuje matematický základ a všeobecné techniky nutné pro implementaci jakéhokoliv mechanismu popsaného v dalších částech ISO/IEC 15946.

Cílem tohoto dokumentu je uspokojit rostoucí zájem o technologie s veřejným klíčem založené na eliptických křivkách a popsat komponenty, které jsou nutné pro implementaci systému bezpečného digitálního podpisu založeného na eliptických křivkách. Jsou popsána schémata pro výměnu klíčů, transport klíčů a digitální podpisy, které jsou založeny na problému diskrétních logaritmů eliptických křivek.

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že vyhovění této mezinárodní normě může

zahrnovat použití patentů.

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu těchto patentových práv.

Držitelé těchto patentových práv ujistili ISO a IEC, že jsou ochotni dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu jsou prohlášení držitelů těchto patentovaných práv registrována u ISO a IEC. Informace lze získat u:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD 8) "*Patent Information*"

SD 8 je veřejně dostupný na: http://www.din.de/ni/sc27

Je třeba upozornit na to, že některé prvky této mezinárodní normy mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

---

1 Předmět normy

Mezinárodní norma ISO/IEC 15946 specifikuje kryptografické techniky s veřejným klíčem založené na eliptických křivkách. Tyto techniky zahrnují ustavení klíčů pro systémy s tajným klíčem a mechanismy digitálního podpisu.

Tato část ISO/IEC 15946 popisuje matematický základ a všeobecné techniky nezbytné pro implementaci kteréhokoliv mechanismu popsaného v dalších částech ISO/IEC 15946.

Předmět této normy je omezen na kryptografické techniky založené na eliptických křivkách definovaných nad konečnými poli mocnin řádu prvočísel (včetně speciálních případů řádu prvočísel s charakteristikou dvě). Reprezentace prvků vlastních konečných polí (tj. jejichž báze je použita) je mimo rozsah této normy.

Mezinárodní norma ISO/IEC 15946 nespecifikuje implementaci technik, které definuje. Není tedy zaručena interoperabilita produktů vyhovujících této mezinárodní normě.

-- Vynechaný text --