ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Srpen**
2006

Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 2: Digitální podpisy	ČSN ISO/IEC 15946-2 36 9794

Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures

Technologies de l´information - Techniques de sécurité - Techniques cryptographiques basées sur les courbes
elliptiques - Partie 2: Signatures digitales

Informationstechnik - IT-Sicherheitsverfahren - Kryptographische Techniken auf Basis von eliptischen Kurven -
Teil 2: Digitale Signaturen

Tato norma je českou verzí mezinárodní normy ISO/IEC 15946-2:2002. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficielní verze.

This standard is the Czech version of the International Standard ISO/IEC 15946-2:2002. It was translated by Czech Standards Institute. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

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

ISO/IEC 15946-1:2002 zavedena v ČSN ISO/IEC 15946-1 (36 9794) Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 1: Všeobecně

Vysvětlivky k textu převzaté normy

Anglický termín „message digest“ je pro účely této normy překládán jako „výtah ze zprávy“.

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 2: Digitální podpisy	ISO/IEC 15946-2 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 společného zájmu. 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 Směrnic ISO/IEC.

Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

ISO/IEC 15946-2 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky*.

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 jsou informativní.

Úvod

Některé z nejzajímavějších a potenciálně užitečných kryptografických systémů s veřejným klíčem, 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 operací „+“, 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 typu Diffie-Hellmana a ElGamala.

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. Skutečně 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 umožňuje použít při výpočtech menší celá čísla.

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.

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)

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

Tato část ISO/IEC 15946 specifikuje kryptografické techniky s veřejným klíčem založené na eliptických křivkách. Tyto techniky zahrnují ustavení klíčů u systémů s tajným klíčem a mechanismy digitálního podpisu.

Tato část ISO/IEC 15946 popisuje mechanismy pro digitální podpisy. Matematický základ a všeobecné techniky nezbytné pro implementaci mechanismů jsou popsány v části 1 ISO/IEC 15946.

Předmět této části ISO/IEC 15946 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 části ISO/IEC 15946.

Tato část ISO/IEC 15946 nespecifikuje plně implementaci technik, které popisuje. K zajištění kompatibility produktů vyhovujících této části ISO/IEC 15946 může být proto požadována další specifikace.

-- Vynechaný text --