ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Říjen**
2006

Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 4: Digitální podpisy umožňující obnovu zprávy	ČSN ISO/IEC 15946-4 36 9794

Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery

Technologies de l´information - Techniques de sécurité - Techniques cryptographiques basées sur les courbes
elliptiques - Partie 4: Signatures digitales offrant un message de recouvrement

Tato norma je českou verzí mezinárodní normy ISO/IEC 15946-4:2004. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 15946-4:2004. 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 9796-3 zavedena v ČSN ISO/IEC 9796-3 (36 9780) Informační technologie - Bezpečnostní

techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech

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

ISO/IEC 14888-1 zavedena v ČSN ISO/IEC 14888 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně

ISO/IEC 15946-1:2002 zavedena v ČSN ISO/IEC 15946-1:2005 (36 9794) Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 1: Všeobecně

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 4: Digitální podpisy umožňující obnovu zprávy	ISO/IEC 15946-4 První vydání 2004-10

ISO copyright office

Case postale 56, CH-1211 Geneva 20

Tel. +41 22 749 01 11

Fax. +41 22 734 10 79

e-mail copyright@iso.ch

Web www.iso.ch

Obsah

Strana

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 2 Směrnic 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.

Mezinárodní norma ISO/IEC 15946-4 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*

Úvod

Potenciálně užitečná třída kryptografických systémů s veřejným klíčem sestává ze schémat založených na eliptických křivkách definovaných nad konečnými poli. Kryptografické systémy s veřejným klíčem založené na eliptických křivkách využívají následující dva poznatky:

– 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 diskrétního umocňování eliptické křivky je možné snadno odvodit obdoby eliptické křivky ze známých schémat s veřejným klíčem Diffie-Hellmana a ElGamala.

Bezpečnost takového systému s veřejným klíčem závisí na obtížnosti určení diskrétních logaritmů v grupě bodů eliptické křivky. Pro podobné velikosti parametrů je tento problém - 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. Proto je 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.

Aby uspokojila rostoucí zájem o technologie s veřejným klíčem založené na eliptických křivkách, definuje tato část ISO/IEC 15946 metody pro implementaci technik digitálního podpisu založených na eliptických křivkách umožňujících obnovu zprávy.

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

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

Předmět této části ISO/IEC 15946 je omezen na kryptografické techniky založené na eliptických křivkách definovaných nad konečnými poli (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 specifikuje pět odlišných mechanismů pro digitální podpisy umožňující obnovu zprávy. Matematický základ a všeobecné techniky nutné pro implementaci mechanismů jsou popsány v ISO/IEC 15946-1.

Mechanismy digitálního podpisu mohou být rozděleny do následujících dvou kategorií.

- Když má být celá zpráva uložena a/nebo přenesena s podpisem, mechanismus se nazývá „mechanismus podpisu s dodatkem“.

- Když může být celá zpráva nebo její část obnovena z podpisu, mechanismus se nazývá „mechanismus podpisu umožňující obnovu zprávy“. Mechanismy specifikované v této části ISO/IEC 15946 spadají do druhé kategorie, tj. umožňují buďto úplnou nebo částečnou obnovu zprávy. [Pro schémata digitálního podpisu s dodatkem založená na eliptických křivkách viz ISO/IEC 15946-2.]

POZNÁMKA V aplikacích, kde je použita k poskytnutí bezpečnostních služeb kombinace algoritmů nebo kde je algoritmus parametrizován volbou kombinace jiných algoritmů, taková kombinace může být specifikována jako posloupnost identifikátorů objektů přiřazených k těmto algoritmům nebo vložením identifikátorů objektů algoritmů nižší úrovně pole parametrů struktury identifikátoru algoritmu specifikujících vyšší úroveň algoritmů (například specifikací identifikátoru objektu hašovací funkce jako parametru ve struktuře identifikátoru algoritmu schématu podpisu). Struktura identifikátoru algoritmu je definována v ISO/IEC 9594-8.

POZNÁMKA Kódování identifikátorů objektů je závislé na aplikaci.

-- Vynechaný text --