Eliptické křivky v kryptografii a mezinárodní normy. Přehled.

Ing. Jaroslav Pinkava, CSc., AEC spol. s r.o., BRNO

1. Úvod

Dnešní kryptografie plní mj. následující základní funkce: *utajení, autentizace, nepopiratelnost, nenarušenost (integrita) zpráv.* Používá k tomu celou škálu prostředků jako jsou šifrovací algoritmy, metody digitálních podpisů, kryptografické protokoly, časové značky (time stamping) a další. Jsou používány dvě základní třídy kryptografických algoritmů: symetrické (především tzv. blokové šifry) a asymetrické (také se jim říká systémy s veřejným klíčem). Řada současných asymetrických kryptosystémů vychází z obtížnosti řešení tří následujících matematických úloh:

- úloha faktorizace velkých čísel (RSA, Rabin-Williams),
- úloha diskrétního logaritmu (např. DSA, Diffie-Hellman),
- úloha eliptického diskrétního logaritmu (ECDSA, eliptické kryptosystémy).

Kryptosystémy s veřejným klíčem umožňují přitom v zásadě trojí typ využití a to jako systémy pro:

- výměnu klíčů pro symetrickou kryptografii
- digitální podpis
- šifrování (obvykle krátkých zpráv, většinou služebního charakteru).

Každý z existujících algoritmů má určité bezpečnostní a implementační vlastnosti, které udávají potom charakter konkrétního řešení, které má k dispozici uživatel. Je potom na navrhovateli, aby zvolil takový systém, který nejlépe odpovídá konkrétním požadavkům. Kryptosystémy na bázi eliptických křivek si přitom zejména v posledních letech vysloužili velkou pozornost díky řadě výhodných vlastností. Mezi ně patří zejména krátká délka klíče při zadaném stupni bezpečnosti kryptosystému (ve srovnání s jinými kryptosystémy s veřejným klíčem), menší nároky na paměť – tj. např. využitelnost při implementacích v prostředí, které klade omezení na velikost použitelné paměti, rychlejší zpracování, menší nároky na spotřebu energie, atd.

Kryptografie se dnes do praxe prosazuje především prostřednictvím celé škály norem, doporučení, standartů. Kryptosystémy na bázi eliptických křivek jsou již součástí celé řady takovýchto norem. V práci je proto proveden jejich určitý přehled. Cílem práce je rovněž provést určitý celkový přehled problematiky, zejména dát k dispozici existující zdroje v literatuře a na Internetu.

2. Základní matematické operace

Pro realizaci eliptických kryptosystémů jsou využívány především dva základní typy těles. Jednak to jsou tělesa prvočíselná (operace probíhají mod p, kde p je prvočíslo), jednak jsou to tělesa binární (resp. se jim také říká tělesa charakteristiky dva - operace probíhají mod 2^n, n je přirozené číslo – dnes je doporučováno používat jako n rovněž pouze prvočísla).

Pro efektivnost konkrétních implementací eliptických kryptosystémů existuje celá řada postupů a technik (lit. [2], [10], [11], [12], [13]). Jedná se např. o metody vyjádření jednotlivých prvků binarních těles (normální resp. polynomiální baze), algoritmy pro sčítání bodů, resp. násobení bodů číslem – kromě klasických technik jsou zde využívány také tzv. projektivní souřadnice atd. Existují určité techniky umožňující optimalizovat příslušné matematické postupy (např. v lit. [10]) a dosáhnout tak efektivní implementace eliptických kryptosystémů.

3. Bezpečnost eliptických kryptosystémů

Bezpečnost eliptických kryptosystémů souvisí s možnostmi řešení úlohy diskrétního logaritmu. Zde existuje několik algoritmů, jejichž výpočetní složitost lze popsat ve tvaru druhé odmocniny z N, kde N je počet bodů příslušné eliptické křivky. Jsou to zejména Pollardova ρ-metoda a Pollardova λ-metoda. Složitost z nich nejefektivnější Pollardovy ρ-metody je daná výrazem $(\pi N/4)^{1/2}$.

Obecně pro řešení úlohy eliptického diskrétního logaritmu není znám žádný algoritmus mající subexponenciální výpočetní složitost jako je tomu pro řešení úlohy faktorizace (RSA) nebo řešení úlohy

klasického diskrétního logaritmu. Existují však určité speciální případy (speciální typy eliptických křivek), kde takovéto postupy existují. Např. v roce 1991 pánové Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone přišli se subexponenciálním algoritmem pro tzv. supersingulární eliptické křivky (MOV útok) a v roce 1997 byl nalezen algoritmus s lineární (!) výpočetní složitostí pro eliptické křivky s tzv. stopou-1 (trace-1). Podobné útoky jsou stále předmětem úvah odborníků, jsou však obvykle orientovány na speciální případy eliptických křivek.

Z tohoto důvodu je také v současnosti doporučováno používat eliptické křivky s náhodně generovanými parametry, kde pravděpodobnost existence podobných útoků je minimální. Zejména atraktivním postupem je možnost generovat parametry eliptické křivky tzv. prokazatelně náhodně. Konstruktér eliptické křivky se takto může vyhnout potenciálním obviněním ze strany uživatele, že vložil do hodnot parametrů určitá zadní vrátka, která mu umožňuji proniknout snadněji za bezpečnostní hranice systému.

Problematikou bezpečnosti eliptických křivek se zabývají např. články [6] resp. [8]. Existující algoritmy pro výpočet diskrétního logaritmu jsou velmi dobře popsány v knize [2].

4. Schoofův algoritmus

Pro konstrukci eliptických křivek je nezbytné pro stanovení konkrétních hodnot parametrů mít k dispozici prostředek pro výpočet počtu bodů dané eliptické křivky. Obecně toto řeší tzv. Schoofův algoritmus.

Hasseho věta (např. v lit [2]) nám říká, že počet bodů eliptické křivky E_q je dán výrazem

$$\text{card } E_q = q + 1 - t,$$

kde $|t| \leq 2\sqrt{q}$. Toto číslo t je však i při zadaných hodnotách základních parametrů eliptické křivky předem neznámé a je třeba výpočtem stanovit jeho hodnotu. Schoofův algoritmus to řeší tak, že počítá t mod L, kde L jsou některá prvočísla (jejich velikost je shora omezená určitou mezí L_{max}). Použitím čínské věty o zbytcích je pak jednoznačně spočtena hodnota t.

Samotný algoritmus má výpočetní složitost $O(\log^8 q)$. Jeho implementace však není zdaleka triviální záležitostí. Aby byla dosažena tato (nízká) výpočetní složitost, je třeba použít složitějších technik založených na poměrně hlubokých výsledcích z teorie čísel.

5. Materiál P1363

Tento materiál je dnes vlastně základem při budování všech novějších norem pro kryptosystémy s veřejným klíčem. Byl zpracováván širokým kolektivem světových odborníků po celou řadu let, v letošním roce (2000) má být schválen v podobě normy.

Jeho součástí je rovněž široký popis aparátu eliptických kryptosystémů. V hlavním dokumentu jsou nejprve uvedeny následující základní pojmy:

Kryptografická rodina (cryptographic family): v normě jsou prezentovány tři základní rodiny kryptografických zobrazení, která jsou založena na následujících (matematicky obtížných) problémech: diskrétní logaritmus v konečném poli (DL), diskrétní logaritmus v grupách eliptických křivek (EC) a na faktorizaci celých čísel (IF).

Parametry systému (**domain parameters):** informace o matematických objektech (jako tělesa či grupy) v jejichž kontextu existují dvojice veřejný a soukromý klíč. Více dvojic klíčů může mít tytéž systémové parametry.

Platné parametry systému (valid domain parameters): taková množina systémových parametrů, která splňuje navíc příslušné specifické matematické požadavky týkající se příslušných parametrů systému pro danou rodinu.

Platný klíč (valid key): klíč (soukromý či veřejný), který splňuje navíc příslušné specifické matematické požadavky klíčů pro danou rodinu.

Platná dvojice klíčů (valid key pair):dvojice veřejný a soukromý klíč, která splňuje navíc příslušné specifické matematické požadavky, kladené na dvojici klíčů pro danou rodinu.

Ověření platnosti (validation): proces, během něhož proběhne ověření platnosti klíče, dvojice klíčů či systémových parametrů.

Základní model:

Následující tříúrovňový model dává potřebnou abstrakci k rozlišení různých typů kryptografických technik:

- Primitivy - základní matematické operace. Tyto historicky vznikly z obtížných problémů teorie čísel. Primitivy samy o sobě nejsou určeny k získání hledané bezpečnosti, ale slouží jako stavební prvky pro schémata.

- Schémata – operace kombinující primitivy a doplňkové techniky (viz dále). Schémata mohou zajistit příslušnou bezpečnost (teoretické hledisko výpočtové složitosti) pokud jsou vhodně aplikována v protokolech.

- Protokoly – posloupnosti operací, které jsou prováděny více stranami za účelem dosažení určitého bezpečnostního cíle. Protokoly mohou dosáhnout požadovanou bezpečnost, pokud jsou správně implementovány.

Primitivy

Norma definuje následující primitivy:

— Odvození tajné hodnoty (Secret Value Derivation Primitives = SVDP) ve schématech pro dohodu na klíči.
— Podpis (Signature Primitives = SP) a verifikace podpisu (Verification Primitives = VP), součásti podpisových schémat.
— Šifrování (Encryption Primitives = EP) a dešifrování (Decryption Primitives = DP), součásti šifrovacích schémat.

Schémata

Norma definuje následující schémata:

— Schéma pro dohodu na klíči (Key Agreement Schemes = KAS), kde dvě strany použijí své dvojice veřejný a soukromý klíč resp. další informaci k vytvoření sdíleného tajného klíče.
— Podpisové schéma s přívěškem (Signature Schemes with Appendix = SSA), ve kterém jedna strana podepíše zprávu svým soukromým klíčem a libovolná jiná strana může ověřit tento podpis užitím zprávy, podpisu a veřejného klíče podepsané strany.
— Podpisové schéma s rozkrytím zprávy (Signature Schemes with Message Recovery = SSR), ve kterém jedna strana podepíše zprávu svým soukromým klíčem a libovolná jiná strana může ověřit tento podpis a rozkrýt samotnou zprávu (pokud podpis je verifikován) užitím podpisu a odpovídajícího veřejného klíče podepsané strany.
— Šifrovací schémata (Encryption Schemes = ES), kde libovolná strana může zašifrovat zprávu užitím veřejného klíče přijímající strany a pouze příjemce může zprávu dešifrovat užitím odpovídajícího svého soukromého klíče. Šifrovací schémata lze použít k dohodě na tajném klíči pro symetrickou kryptografii.

Přehled schémat z P1363

Schéma	*Primitiv*	*Doplňková technika*
Schéma pro dohodu na klíči		
DLKAS-DH1	***DLSVDP-DH resp. -DHC***	***KDF1***
ECKAS-DH1	***ECSVDP-DH resp. -DHC***	***KDF1***
DL/ECKAS-DH2	***DL/ECSVDP-DH and/or –DHC***	***KDF1***

DLKAS-MQV	***DLSVDP-MQV resp. - MQVC***	***KDF1***
ECKAS-MQV	***ECSVDP-MQV resp. - MQVC***	***KDF1***
Podpisové schéma s přívěškem		
DLSSA	***DLSP-NR a DLVP-NR resp. DLSP-DSA a DLVP-DSA***	***EMSA1***
ECSSA	***ECSP-NR a ECVP-NR resp. ECSP-DSA a ECVP-DSA***	***EMSA1***
IFSSA	***IFSP-RSA1 a IFVP-RSA1 resp IFSP-RSA1 a IFVP-RSA2 Resp IFSP-RW a IFVP-RW***	***EMSA2***
Podpisové schéma s rozkrytím zprávy		
IFSSR	***IFSP-RSA1 a IFVP-RSA1 resp. IFSP-RSA1 a IFVP-RSA2 resp. IFSP-RW a IFVP-RW***	***EMSR1***
Šifrovací schéma		
IFES	***IFEP-RSA a IFDP-RSA***	***EME1 (hashovací funkce, MGF a OAEP)***

Schémata pro dohodu na klíči

V schématech pro dohodu na klíči kombinuje každá strana svůj soukromý klíč s veřejným klíčem jiné strany za účelem odvození tajného klíče (pro symetrickou šifru). Další pužité informace (veřejné či utajované) se nazývají parametry pro odvození klíče.

DLKAS-DH1/ECKAS-DH1 (Discrete Logarithm and Elliptic Curve Key Agreement Scheme, Diffie-Hellman version) - každá strana má k dispozici jednu dvojici klíčů.

DL/ECKAS-DH2 (Discrete Logarithm and Elliptic Curve Key Agreement Scheme, Diffie-Hellman version) - každá strana má k dispozici dvě dvojice klíčů.

DLKAS-MQV/ECKAS-MQV
(Discrete Logarithm and Elliptic Curve Key Agreement Schemes, Menezes-Qu-Vanstone version)) - každá strana má k dispozici dvě dvojice klíčů.

Podpisová schémata

DLSSA/ECSSA (Discrete Logarithm and Elliptic Curve Signature Schemes with Appendix).

Schémata pro šifrování

EMSA1
EMSA1 je kódovací metoda pro vytváření podpisů s přívěškem založená na hashovací funkci. Je doporučena pro užití spolu s DLSSA a ECSSA. Použitou hashovací funkcí Hash s délkou výstupu *hLen* oktetů by měla být SHA-1 či RIPEMD-160, či technika spojená s užitím pro EMSA1 (příloha normy P1363). Maximální délka zprávy M (oktetový řetězec) je $2^{61} - 1$ oktetů. Výstup (celé nezáporné číslo f, reprezentant zprávy) je omezen na maximální délku I (v bitech), tj. počet jeho bitů je nejvýše min(*l*, 8*hLen*). (Dále jsou v normě ještě uvedeny schémata EMSA2, EMSR1 a EME1).

Příloha Annex A. materiálu P1363 obsahuje celou řadu matematických postupů použitelných při řešení konkrétních implementací. Obsahuje také některé vybrané a spočtené hodnoty parametrů.

6. ANSI X9. 62 a ANSI X9.63

Tyto normy [12] jsou určeny zejména pro finanční sféru. Vychází z práce skupiny P1363 (předešlý odstavec). Řadu otázek přitom již řeší konkrétněji (zejména např. podpisové schéma ECDSA) a s větším ohledem na praktické realizace. Součástí materiálu jsou i některé vybrané a spočtené hodnoty parametrů.

7. SECG

Zpracování těchto materiálů (lit. [13] – http://www.secg.com) iniciovala firma Certicom. Zabývají se řadou konrétních otázek souvisejících s implementacemi eliptických kryptosystémů. Významnou je zejména doporučená množina vybraných parametrů pro eliptické křivky.

8. NIST

Materiál zpracovává doporučenou množinu vybraných parametrů pro eliptické křivky pro užití ve státní a veřejné správě v USA

9. Některé další normy (ISO, IETF)

V materiálech [15] - [18] jsou popsány další standardizované postupy při implementacích eliptických křivek.

10. Citovaná literatura

[1] Atkin, A.O.L.; Morain, F.: Elliptic Curves and primality proving, Math. Comp., 61, 29-67, 1993
[2] Blake, I.F.; Seroussi, G.; Smart, N.P.: *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series 265, Cambridge, University Press 1999, 204 +20 pp.
[3] Koblitz, Neal: Elliptic curve cryptosystems, Math. Comúp., 48, 203-209, 1987
[4] Koblitz, N. *A course in number theory and cryptography*, Graduate Texts in Mathematics **114**, Springer-Verlag, 2nd edition, 1994.
[5] Koblitz, Neal: Algebraic Aspects of Cryptography, Springer-Verlag, Berlin 1998, 206+10 pp.
[6] Lenstra, Arjen K.; Verheul, Eric R.: Selecting Cryptographic Key Sizes, November 1999 (Internet)

[7] Pinkava, J.: What is going on in the world of cryptography?, in: INFO´99: Internetanwendungen für den Mittelstand, Dr. Wilke GmbH Verlag, Berlin 1999, 283-287
[8] Pinkava, J.: Jak je to s bezpečností eliptických kryptosystémů?, CryptoWorld 11/99
[9] Miller, V.: Use of elliptic curves in cryptography, Advances in Cryptology, Crypto 85, 417-426
[10] Rosing, M.: *Implementing Elliptic Curve Cryptography*, Manning 1999, 316+14 pp.
[11] P1363 – IEEE P1363 / D11 (Draft Version 11): Standard Specifications for Public Key Cryptography
[12] ANSI X9.62: Accredited Standards Committee X9. *The Elliptic Curve Digital Signature Algorithm*
ANSI X9.63: Accredited Standards Committee X9. *Key Agreement and Key Management Using Elliptic Curve-Based Cryptography*
[13] SECG drafts: SEC 1 - Elliptic Curve Cryptography (version 0.5)
SEC 2 - Recommended elliptic curve domain parameters (version 0.6)
GEC 2 - Test Vectors for SEC 1 (version 0.3)
ECC X.509 Specification
[14] National Institute of Standards and Technology. June 1999 - Recommmended Elliptic Curves For Federal Government Use
[15] Elliptic Curve S/MIME, draft-ietf-smime-ecc-00.txt
[16] PKCS 13: *Elliptic Curve Cryptography Standard* (RSA Laboratories, in preparation)
[17] Internet X.509 Public Key Infrastructure Representation of Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and Signatures in Internet X.509 Public Key Infrastructure Certificates, draft-ietf-pkix-ipki-ecdsa-02.txt
[18] ISO/IEC 15946-1. *Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: Genera*l. 1998. Working draft.
ISO/IEC 15946-2. *Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signature*s. 1998. Working draft.
ISO/IEC 15946-3. *Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 3: Key establishmen*t. 1998. Working draft.
ISO/IEC FCD 14888-3: Digital signatures with appendix – Part 3: Certificate-based mechanisms. Status: Final Committee Draft;

11. Další literatura (publikace dostupné na webu)

Poznámka. Velmi dobrou (a zatím stále ještě aktuální) bibliografii k eliptickým křivkám lze nalézt v knize[2].

[W1] A. O. L. Atkin and F. Morain: Elliptic curves and primality proving, Math. Comp. 61, 203, july 1993, pp. 29-68. Abstract: This report describes the theory and implementation of the Elliptic Curve Primality Proving algorithm -- ECPP -- algorithm. This includes the relationships between representing primes by quadratic forms and the explicit construction of class fields of imaginary quadratic fields; the theory of elliptic curves with complex multiplication over the field of complex numbers as well as over finite fields. We then use this theory to design a very powerful primality proving algorithm. Half of the paper is devoted to the description of its implementation. In particular, we give the currently best algorithms to speed up each part of the program. The resulting program is very fast. We can prove the primality of 100-digit numbers in less than five minutes on a SUN 3/60 workstation, and we can treat all numbers with less than 1000 digits in a reasonable amout of time using a distributed implementation.

[W2] A. O. L. Atkin and F. Morain: Finding suitable curves for the elliptic curve method of factorization, Math. Comp., 60, 201, january 1993, pp. 399-405.
Using the parametrizations of Kubert, we show how to produce infinite families of elliptic curves which have prescribed nontrivial torsion over Q and rank at least one. These curves can be used to speed up the ECM factorization algorithm of Lenstra. We also briefly discuss curves with complex multiplication in this context.

[W3] Beauregard, Dan: Efficient Algorithms for Implementing Elliptic Curve Public-Key Schemes, Faculty of the Worchester Polytechnic Institute, May 1996, 96 pp.

[W4] Guang Gong, Thomas A. Berson; Douglas R. Stinson: Eliptic Curve Pseudorandom Sequence Generators, 21 pp.

[W5] Johannes Buchmann, Volker Müller: Computing the number of points on elliptic curves over finite prime fields, (ISSAC 1991)

[W6] Johannes Buchmann; Damian Weber: Discrete Logarithms: Recent Progress, 19 pp.
Abstract: We summarize recent developments on the computation of discrete logarithms in general groups as well as in some specialized settings. More specifically, we consider the following abelian groups: the multiplicative group of finite fields, the group of points of an elliptic curve over a finite field, and the class group of quadratic number fields.

[W7] J.-M. Couveignes and F. Morain: Schoof's algorithm and isogeny cycles , appeared in Proc. ANTS-I, Lecture Notes in Computer Science 877, 1994, pp. 43-58.
Abstract: The heart of Schoof's algorithm for computing the cardinality m of an elliptic curve over a finite field is the computation of m modulo small primes l. Elkies and Atkin have designed practical improvements to the basic algorithm, that make use of "good" primes l. We show how to use powers of good primes in an efficient way. This is done by computing isogenies between curves over the ground field. A new structure appears, called "isogeny cycle". We investigate some properties of this structure.

[W7] J.-M. Couveignes, L. Dewaghe and F. Morain: Isogeny cycles and the Schoof-Elkies-Atkin algorithm, Rapport de recherche LIX/RR/96/03, submitted for publication.
Abstract: The heart of Schoof's algorithm for computing the cardinality m of an elliptic curve over a finite field is the computation of m modulo small primes l. Elkies and Atkin have designed practical improvements to the basic algorithm, that make use of ``good'' primes l. We show how to use powers of good primes in an efficient way. This is done by computing isogenies between curves over the ground field. We investigate the properties of the ``isogeny cycles'' that appear.

[W8] Djabri, Z.; Smart, N.P.: A Comparison of Direst and Indirect Methods for Computing Selmer Groups of an Elliptic Curve,

[W9] Galbraith, S.: Jacobians of Hyperelliptic Curves, 10 pp.

[W10] Galbraith, S.: On the relationship between the discrete logarithm problems on isogenous elliptic curves

[W11] Galbraith, Steven: Eliptic Curve Cryptosystem project, First Meeting Friday January 24th 1997, 4 pp.
Abstract: discussed the absolute basics of the theory of elliptic curves over finite fields and showed how Diffie-Hellman key exchange may be implemented with elliptic curves.

[W12] Galbraith, S.; Paulus, S.; Smart, N.P.: Arithmetic on superelliptic curves, 21 pp.

[W13] Robert Gallant, Robert Lambert, and Scott Vanstone: Improving the Parallelized Pollard Lambda Search on Binary Anomalous Curves
ABSTRACT: The best algorithm known for finding logarithms on an elliptic curve (E) is the (parallelized) Pollard lambda collision search. We show how to apply a Pollard lambda search on a set of equivalence classes derived from E, which requires fewer iterations than the standard approach. In the case of binary anomalous curves over $F_{2}m$, the algorithm speeds up the standard algorithm by a factor $sqrt{2m}$.

[W14] J. Guajardo, C. Paar, " Efficient Algorithms for Elliptic Curve Cryptosytems", CRYPTO '97, August 17-21, Santa Barbara, CA, USA.

[W15] J. Guajardo, C. Paar, "Efficient Algorithms for Elliptic Curve Cryptosytems," CRYPTO '97, August 17-21, Santa Barbara, CA, USA.

[W16] J. Guajardo, C. Paar, "Speeding Up Inversion in Composite Galois Fields," 1998 IEEE International Symposium on Information Theory, August 16-21, 1998, MIT, Cambridge, MA, USA.

[W17] Jorge Guajardo, " Efficient Algorithms for Elliptic Curve Cryptosystems", Master's Thesis, Worcester Polytechnic Institute, May 1997.
Abstract: Elliptic curves are the basis for a relative new class of public-key schemes. It is predicted that elliptic curves will replace many existing schemes in the near future. It is thus of great interest to develop algorithms which allow efficient implementations of elliptic curve crypto systems. This thesis deals with such algorithms.

Efficient algorithms for elliptic curves can be classified into low-level algorithms, which deal with arithmetic in the underlying finite field and high-level algorithms, which operate with the group operation. This thesis describes three new algorithms for efficient implementations of elliptic curve cryptosystems. The first algorithm describes the application of the Karatsuba-Ofman Algorithm to multiplication in composite fields GF((2n)m). The second algorithm deals with efficient inversion in composite Galois fields of the form GF((2n)m). The third algorithm is an entirely new approach which accelerates the multiplication of points which is the core operation in elliptic curve public-key systems. The algorithm explores computational advantages by computing repeated point doublings directly through closed formulae rather than from individual point doublings. Finally we apply all three algorithms to an implementation of an elliptic curve system over GF((216)11). We provide ablolute performance measures for the field operations and for an entire point multiplication. We also show the improvements gained by the new point multiplication algorithm in conjunction with the k-ary and improved k-ary methods for exponentiation.

[W18] Hamdy, Safuat: Anwendungen elliptischer Kurven in der Kryptologie, (http://www.informatik.uni-hamburg.de/TGI/studenten/hamdy/deutsch/veroeffentlichungen.html)

[W19] Y. Zheng and H. Imai, Efficient Signcryption Schemes On Elliptic Curves; Proceedings of the IFIP 14th International Information Security Conference (IFIP/SEC'98), Chapman & Hall, September 1998, Vienna, Austria.

[W20] Marc Joye and Jean-Jacques Quisquater: Note on the preliminary version of Meyer and Müller's cryptosystem, Tech. Report CG-1996/2, UCL Crypto Group, Louvain-la-Neuve, January 29, 1996
Abstract: After the introduction of RSA cryptosystem, Rabin proposed to use even exponents. The resulting function was four-to-one, and was proved as intractable as factorization. Shortly after, Williams showed how to transform the Rabin's function to a one-to-one. More recently, Meyer and Müller proposed an analogous cryptosystem based on elliptic curves over a ring. We will show that their cryptosystem is equivalent to the Williams'one in terms of security.

[W21] Marc Joye and Jean-Jacques Quisquater: Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams, Presented at the rump session of Eurocrypt'96, Zaragoza (Spain), 12-16th May 1996, To appear in Designs, Codes and Cryptography
Abstract: In an earlier work, we showed that the preliminary version of the Meyer-Müller's cryptosystem may be reduced to the one of Rabin-Williams. In this paper, we prove that the second version of their cryptosystem may also be reduced to the cryptosystem of Rabin-Williams.

[W22] Marc Joye: Introduction élémentaire a la théorie des courbes elliptiques, 1995, 77 pp.

[W23] Marc Joye and Jean-Jacques Quisquater: Reducing the elliptic curve cryptosystem of Meyer-Muller to the cryptosystem of Rabin-Williams, Designs, Codes and Cryptography, Vol. 14, No. 1, pp. 53-56, 1998.
Abstract. In an earlier work, we showed that the preliminary version of the Meyer-Muller's cryptosystem may be reduced to the one of Rabin-Williams. In this paper, we prove that the second version of their cryptosystem may also be reduced to the cryptosystem of Rabin-Williams.

[W24] Counting the number of points of on elliptic curves over finite fields: strategies and performances , R. Lercier and F. Morain, appeared in Proc. Eurocrypt '95, Lecture Notes in Computer Science 921, Springer, 1995, pp. 79-94.
Cryptographic schemes using elliptic curves over finite fields require the computation of the cardinality of the curves. Dramatic progress have been achieved recently in that field by various authors. The aim of this article is to highlight part of these improvements and to describe an efficient implementation of them in the particular case of the fields GF(2^n), for n <= 600.

[W25] R. Lercier and F. Morain: Algorithms for computing isogenies between elliptic curves, preprint.

[W26] R. Lercier and F. Morain:Counting points on elliptic curves over F(p^n) using Couveignes's algorithm, submitted version (version 96/01/25).
Abstract: The heart of the improvements of Elkies to Schoof's algorithm for computing the cardinality of elliptic curves over a finite field is the ability to compute isogenies between curves. Elkies' approach was well suited for the case where the characteristic of the field is large. Couveignes showed how to compute isogenies in small characteristic. The aim of this paper is to describe the first successful implementation of Couveignes's algorithm

and to give numerous computational examples. In particular, we describe the use of fast algorithms for performing incremental operations on series. We will also insist on the particular case of the characteristic 2.

[W27] James McKee; R. Pinch: On a cryptosystem of Vanstone and Zuccherato,
Abstract: Vanstone and Zuccherato proposed a public-key elliptic curve cryptosystem in which the public key consists of an integer N and an elliptic curve E defined over the ring ${\mathbf Z}/N{\mathbf Z}$. Here N is a product of two secret primes p and q, each of special Form, and the order of E modulo N is smooth. We present three attacks, each of which factors the modulus N and hence breaks the cryptosystem. The first attack exploits the special form of p and q; the second exploits the smoothness of the elliptic curve; and the third attack breaks a proposed application of the system to user authentication. For parameters as in \cite{VZ}, the modulus can be factored within a fraction of a second.

[W28] Alfred J. Menezes, Yi-Hong Wu, Robert J. Zuccherato: An elmentary introduction to hyperelliptic curves, November 1996,
Abstract: This paper presents an elementary introduction to some of the theory of hyperelliptic curves over finite filds of arbitrary characteristic that has cryptographic relevance. Cantor´s algorithm for adding in the jacobian of a hyperelliptic curve and a proof of correctness of the algortithm are presented.

[W29] Bernd Meyer, Volker Müller: A Public Key Cryptosystem Based on Elliptic Curves over Z/nZ Equivalent to Factoring (Proceedings if Eurocrypt 1996)

[W30] F. Morain: Isogeny computations and point counting on elliptic curves., slides of a talk given at ECC'98, Waterloo, september 1998

[W31] F. Morain:: Building Cyclic Elliptic Curves Modulo Large Primes, appeared in Proc. Eurocrypt '91, Lecture Notes in Computer Science 547, Springer, 1991, pp. 328-336
Abstract:Elliptic curves play an important rôle in many areas of modern cryptology such as integer factorization and primality proving. Moreover, they can be used in cryptosystems based on discrete logarithms for building one-way permutations. For the latter purpose, it is required to have cyclic elliptic curves over finite fields. The aim of this note is to explain how to construct such curves over a finite field of large prime cardinality, using the ECPP primality proving test of Atkin and Morain.

[W32] F. Morain: Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm, INRIA Research Report 911, october 1988.
Abstract: We describe a primality testing algorithm, due essentially to Atkin, that uses elliptic curves over finite fields and the theory of complex multiplication. In particular, we explain how the use of class fields and genus fields can speed up certain phases of the algorithm. We sketch the actual implementation of this test and its use on testing large primes, the records being two numbers of more than 550 decimal digits. Finally, we give a precise answer to the question of the reliability of our computations, providing a certificate of primality for a prime number.

[W33] F. Morain: Easy numbers for the Elliptic Curve Primality Proving Algorithm, in Paul S. Wang, editor, ISSAC '92, pages 263--268, New York, 1992. ACM Press. Proceedings, July 27--29, Berkeley.
Résumé: We present some new classes of numbers that are easier to test for primality with the Elliptic Curve Primality Proving algorithm than average numbers. It is shown that this is the case for about half the numbers of the Cunningham project. Computational examples are given.

[W34] F. Morain: Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques, appeared in J. Théor. Nombres Bordeaux, 7, 1995, p. 255--282.
Abstract: We describe the algorithms that are needed for an efficient implementation of Schoof's method for computing the number of points on en elliptic curve over a finite field. We try to unify the ideas of Atkin and Elkies. In particular, we describe the computation of equations for X0(l), l a prime number, as well as the efficient computation of factors of the division polynomials of an elliptic curve.

[W35] F. Morain: THESE: Courbes elliptiques et tests de primalité Thèse, Université de Lyon I, 20 septembre 1990. It contains several chapters, some of which are:
Contents. 1. Introduction. 2. Some properties of quadratic forms and fields. 3. Modular forms. 4. Elliptic curves. 5. Primality testing. 6. Analysis. 7. Strategies. 8. Precomputetion. 9. Implementation details. 10Numerical results. 11. What proof do we get? 12. Conclusion., 50 pp. (23-72)
Chapter 2: On Cornacchia's algorithm, F. Morain and J.-L. Nicolas. , 10 pp. (75-86)

Chapter 3.1: Construction of Hilbert class fields of imaginary quadratic fields and dihedral equations modulo p. , 12 pp. (87-98)
Chapter 3.2: Solving equations of small degree modulo large primes. , 14 pp. (101-114)
Chapter 4: Speeding up the computations on an elliptic curve using addition-subtraction chains, F. Morain et J. Olivos, published in RAIRO Inform. Théor. Appl., 1990, 24, 6, p. 531-543. , 12 pp. (119-130)
Chapter 5: Using a programmable gate array in modular arithmetic. , 14 pp. (133-146)
Chapter 6: Atkin's test: news from the front, published in the Proceedings of EUROCRYPT '89, Lecture Notes in Comput. Sci. 434. , 12 pp. (151-163)
Chapter 7: Elliptic curves, primality proving and some Titanic primes, published in the comptes-rendus des Journées Arithmétiques 1989, Astéristque vol 198--199-200. , 6 pp. (165-170)
Chapter 8: Distributed Primality Proving and the primality of (2^3539+1)/3, published in the Proceedings d'EUROCRYPT '90, Lecture Notes in Comput. Sci. 473. , 14 pp. (173-186)
New references. Bugs., 1 pp.

[W36] R.G.E. Pinch: Extending the Wiener attack to RSA-type cryptosystems, Electronics Letters, 31, no. 20 (28 Sep 1995) 1736--1738
Abstract: We show that the attack of Wiener on RSA cryptosystems with a short deciphering exponent extends to systems using other groups such as elliptic curves, and {\smc Luc}.

[W36] Silverman, Joseph H.; Suzuki, Joe: Elliptic curve discrete logarithms and the index calculus, AsiaCrypt '98,

[W37] Silverman, Joseph H.: Rational Points on Elliptic Surfaces
(A talk at the Newton Institute, March 31, 1998)

[W38] Silverman, Joseph H.: A survey of the arithmetic theory of elliptic curves, Modular Forms and Fermat's Last Theorem, Springer, 1997

[W39] Silverman, Joseph H.: The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem

12. Některé webovské stránky zabývající se problematikou eliptických křivek v kryptografii.

http://www.certicom.ca/ecc/enter/index.htm
http://www.cryptomathic.dk/elliptic/elliptic.html
http://www.rzuser.uni-heidelberg.de/~hb3/ellc.html
http://www.geocities.com/CapeCanaveral/Launchpad/9160/biblio_ell.html
http://www.eleves.ens.fr:8080/home/fermigie/elliptic.html.en
http://ds.dial.pipex.com/george.barwood/ec_faq.htm
http://www.math.uni-augsburg.de/~enge/Krypto.html
http://www.math.jussieu.fr/~fermigie/elliptic.html.fr
http://www.cs.rhbnc.ac.uk/~stevenga/ecc.html