Implementação eficiente em *software* de curvas elípticas e emparelhamentos bilineares

Diego F. Aranha[1], **Julio López (Orientador)**[1]

[1] Instituto de Computação – Universidade Estadual de Campinas (UNICAMP)

{dfaranha,jlopez}@ic.unicamp.br

Abstract. *The development of asymmetric or public key cryptography made possible new applications of cryptography such as digital signatures and electronic commerce. Elliptic Curve Cryptography is among the most efficient public-key methods because of its low storage and computational requirements. The relatively recent advent of Pairing-Based Cryptography allowed further constructions of flexible and innovative cryptographic solutions. However, the computational cost of pairing-based cryptosystems remains significantly higher than traditional public key cryptosystems and thus an important obstacle for adoption, specially in resource-constrained devices. The main contributions of this work aimed to improve the performance of curve-based cryptosystems, consisting of efficient formulation and implementation of finite field arithmetic in different computing platforms; and serial and parallel algorithmic techniques for arithmetic in elliptic curves and computation of cryptographic pairings. These contributions produced important performance improvements and several speed records for computing relevant cryptographic algorithms in modern computer architectures ranging from embedded 8-bit microcontrollers to 8-core processors.*

Resumo. *O advento da criptografia assimétrica ou de chave pública possibilitou a aplicação de criptografia na forma de assinaturas digitais e comércio eletrônico. Dentre os vários métodos de criptografia assimétrica, a Criptografia de Curvas Elípticas destaca-se pelos baixos requisitos de armazenamento e custo computacional para execução. A descoberta relativamente recente da criptografia baseada em emparelhamentos bilineares permitiu ainda sua flexibilização e a construção de sistemas criptográficos com propriedades inovadoras. Porém, o custo computacional de sistemas baseados em emparelhamentos ainda permanece significativamente superior aos tradicionais, representando um obstáculo para sua adoção, especialmente em dispositivos com recursos limitados. As contribuições deste trabalho objetivaram aprimorar o desempenho de sistemas baseados em curvas elípticas e emparelhamentos bilineares e consistem em formulação e implementação eficientes de aritmética em corpos finitos em diversas plataformas computacionais; técnicas algorítmicas seriais e paralelas para aritmética em curvas elípticas e cálculo de emparelhamentos de interesse criptográfico. Estas contribuições permitiram obter significativos ganhos de desempenho e uma série de recordes de velocidade para o cálculo de diversos algoritmos criptográficos relevantes em arquiteturas modernas que vão de sistemas embarcados de 8* bits *a processadores com 8* cores.

[1]Financiado por FAPESP, Processo No. 2007/06950-0.

1. Introdução

A descoberta da criptografia de chave pública [1] revolucionou a forma de se construir sistemas criptográficos e possibilitou, de forma definitiva, a integração entre teoria criptográfica e implementação em aplicações reais. Em particular, trouxe a possibilidade de se estabelecer serviços criptográficos como sigilo e assinatura irretratável em ambientes onde não existe qualquer relação de confiança entre os envolvidos ou canal seguro para distribuição de chaves. O surgimento de infra-estruturas de chaves públicas solucionou o problema de tituaridade de chaves públicas e impulsionou o comércio eletrônico. Por outro lado, criou diversos problemas adicionais, durante operações de validação de certificados e revogação de chaves públicas. A descoberta de sistemas criptográficos baseados no problema do logaritmo discreto em curvas elípticas [2, 3] produziu uma nova revolução na área. Ao apresentarem desempenho superior e exigirem chaves mais curtas para um mesmo nível de segurança que os métodos tradicionais de criptografia assimétrica, especialmente o algoritmo RSA [4], alguns dos problemas inerentes às infra-estruturas de chaves públicas foram minimizados. Contudo, a dificuldade de gerência e a sobrecarga de desempenho decorrentes da utilização de certificados ainda impõe obstáculos na adoção de criptografia assimétrica em ambientes restritos.

A busca de alternativas ao paradigma tradicional de infra-estruturas de chave pública resultou na descoberta de sistemas criptográficos baseados em identidade. A motivação original para esses sistemas baseados era aproveitar a autenticidade de informação publicamente conhecida para simplificar a autenticação de chaves públicas. Foram concebidos inicialmente em 1984, para assinaturas digitais, mas as primeiras realizações funcionais e eficientes para cifração só foram apresentadas em 2001, a partir de emparelhamentos bilineares sobre curvas elípticas. Após esta aplicação de emparelhamentos, uma gama de novos protocolos com propriedades inovadoras e especiais foi desenvolvida, flexibilizando as primitivas criptográficas conhecidas e ampliando os cenários de aplicação de criptografia assimétrica.

2. Justificativa e objetivo

Apesar das propriedades inovadoras, o desempenho de sistemas criptográficos baseados em emparelhamentos ainda é uma limitação. Por essa razão, este projeto teve como finalidade desenvolver algoritmos eficientes (seqüenciais e paralelos) e implementações em *software* otimizadas para criptografia baseada em emparelhamentos e curvas elípticas. Vários níveis de aritmética foram acelerados: cálculo do emparelhamento propriamente dito, aritmética na curva elíptica onde o emparelhamento encontra-se definido, aritmética no corpo finito onde a curva elíptica está definida e aritmética nas extensões algébricas deste corpo.

O objetivo principal deste trabalho consistiu em tornar estes métodos de criptografia mais eficientes nas arquiteturas modernas, abrangendo tanto pesquisa algorítmica quanto pesquisa aplicada de implementação. A implementação exigiu o projeto de técnicas de otimização de algoritmos em arquiteturas modernas (embarcadas, multiprocessadas) e concretizou os algoritmos em código funcional eficiente, fazendo o melhor uso possível dos recursos disponibilizados pelo *hardware*. Para isso, paralelismo em nível de tarefas e em nível de dados foram extensamente utilizados, incluindo a aplicação de multiprocessamento e conjuntos de instruções vetoriais como as famílias SSE e AVX.

3. Contribuições

Esta seção apresenta uma relato em duas partes dos resultados obtidos: implementação de criptografia de curvas elípticas e de criptografia baseada em emparelhamentos bilineares.

3.1. Implementação de criptografia de curvas elípticas

O primeiro conjunto de resultados foi derivado da implementação de corpos e curvas elípticas binárias em sensores sem fio. O baixo poder computacional dos sensores torna inviável a utilização de algoritmos convencionais de criptografia de chave pública (RSA, por exemplo) e, até recentemente, primitivas de segurança como sigilo, autenticação e integridade eram alcançadas apenas através de técnicas de criptografia simétrica. Nos artigos [5, 6, 7] publicados como resultados da tese, são apresentadas técnicas para implementação de aritmética em corpos binários em microcontroladores AVR ATmega de 8 *bits* que aproveitam ao máximo os recursos da plataforma subjacente em busca de desempenho. A implementação de curvas elípticas no nível de segurança de 80 *bits* sobre estes corpos permite calcular uma multiplicação de ponto aleatório, operação fundamental de protocolos baseados em curvas elípticas, em menos de $\frac{1}{3}$ segundo. Este resultado contraria diversas observações levantadas em trabalhos anteriores sobre a inviabilidade de curvas binárias para dispositivos limitados, e aperfeiçoa o estado-da-arte entre 57% e 61%. As otimizações desenvolvidas podem também ser empregadas em outras arquiteturas com conjunto de instruções limitado e latência proibitiva em operações de acesso à memória, típicas do segmento de microcontroladores.

O segundo conjunto de resultados trata da implementação de corpos binários em conjuntos de instruções vetoriais. Em particular, havia interesse em se aproveitar explicitamente instruções de permutação de *bytes* que codificam implicitamente acessos simultâneos a tabelas de constantes. Foi desenvolvida uma formulação da aritmética com granularidade de 4 *bits* que emprega vastamente as instruções de permutação, produzindo inclusive um novo ainda que ineficiente algoritmo de multiplicação. Esta formulação foi complementada com um estudo detalhado dos impactos algorítmicos da disponibilidade repentina de suporte nativo à multiplicação em um corpo binário recentemente introduzida na arquitetura Intel. A aceleração significativa da operação de multiplicação forçou uma reavaliação de estratégias de implementação para a operação de multiplicação de ponto em curvas elípticas binárias e sua paralelização em múltiplas unidades de processamento. Estes resultados são apresentados nos artigos [8, 9, 10]. O primeiro trabalho obtém ganhos de desempenho entre 8% e 84% para diversas operações em um corpo binário. Esta formulação eficiente da aritmética permitiu aprimorar o estado da arte para multiplicação de ponto em 27%-30%, desconsiderando o modo de operação em lote. O custo médio de uma multiplicação de ponto em modo lote no nível de segurança de 128 *bits* foi superado em 10% apenas nos dois últimos trabalhos, após a introdução de suporte nativo à multiplicação em um corpo binário. Estes últimos apresentam ainda resultados experimentais para implementações seriais e paralelas da operação de multiplicaçao de ponto nos níveis de segurança de 112, 128 e 192 *bits*.

3.2. Implementação de criptografia baseada em emparelhamentos bilineares

Em seguida, buscou-se estudar protocolos úteis para o fornecimento de serviços de segurança em redes de sensores sem fio. Um exemplos com estas características é um protocolo de

acordo de chaves não-interativo, providenciando o acordo autenticado de chaves simétricas entre nós sensores sem exigir qualquer comunicação, o que permite importante economia de energia. Outro exemplo é o emprego de assinaturas digitais para transmissão autenticada de mensagens entre um nó específico da rede de sensores e um usuário ou aplicação final. Esta linha de pesquisa produziu os resultados [11, 12, 13]. Os dois primeiros trabalhos obtém uma aceleração de até 61% no cálculo do emparelhamento η_T sobre curvas supersingulares binárias a partir de uma generalização das técnicas previamente desenvolvidas. O terceiro trabalho compara a implementação de diversos esquemas de assinatura digital sobre curvas elípticas e emparelhamentos bilineares, fornecendo um panorama completo da relação entre tempo de execução, consumo de memória e consumo de energia. Surpreendentemente, foi detectado que assinaturas curtas não fornecem a economia de energia suficiente em sensores para justificar sua escolha em detrimento de esquemas convencionais.

Dada a tendência tecnológica recente da indústria de computação em migrar as arquiteturas computacionais para arquiteturas paralelas, algoritmos paralelos para cálculo de emparelhamentos em arquiteturas multiprocessadas são desejáveis. Desta forma, foi derivada uma formulação paralela do Algoritmo de Miller [14] empregado para o cálculo de emparelhamentos bilineares. Esta formulação fornece um algoritmo genérico independente da instanciação do emparelhamento e com ótima escalabilidade em curvas sobre corpos de característica pequena [15]. Essa construção foi então acelerada com técnicas para implementação de corpos binários em processadores equipados com conjuntos de instruções vetoriais para reduzir sobrecargas da paralelização e produziu aprimoramentos em relação ao estado-da-arte de 28%, 44% e 66% empregando 2, 4 e 8 processadores, respectivamente. A aceleração do cálculo serial foi também significativa e situou-se em pouco mais de 24% [16, 17]. As mesmas técnicas permitiram ainda o estabelecimento de um novo recorde de velocidade para emparelhamentos simétricos com a derivação e implementação de um novo emparelhamento *eta* otimal sobre curvas supersingulares binárias de genus 2 [18]. Para o cálculo de emparelhamentos assimétricos, propomos várias técnicas para sua implementação serial no nível de segurança de 128 *bits* [19]: (i) a generalização da noção de *redução modular preguiçosa* para aritmética em corpos de extensão e em *twists* de curvas elípticas; (ii) o desenvolvimento de novas fórmulas para o cálculo de quadrados comprimidos sucessivos em subgrupos ciclotômicos de corpos de extensão; (iii) a eliminação de penalidades de desempenho em parametrizações negativas de curvas Barreto-Naehrig. Estas novas técnicas estabelecem um novo recorde de velocidade para o cálculo de qualquer emparelhamento, aprimorando o melhor resultado anterior em até 34%. Finalmente, revisitamos o problema do cálculo paralelo de emparelhamentos, aprimorando significativamente os resultados obtidos anteriormente com o emprego dos quadrados comprimidos em grupos ciclotômicos, do suporte nativo à multiplicação binária e de um compromisso entre tempo de execução e espaço de armazenamento para acelerar a exponenciação final do emparelhamento η_T. Além disso, como tentativa de se contornar os obstáculos à paralelização do Algoritmo de Miller, foi proposto um novo emparelhamento baseado no emparelhamento de Weil. Esta nova construção permitiu incrementar a escalabilidade do cálculo do emparelhamento *ate* otimal primo em máquinas com até 8 unidades de processamento [20].

A tese consolidou 15 resultados submetidos ao processo de revisão por pares: 1 trabalho aceito em revista não-indexada por ter sido recentemente fundada na área, 3 trabalhos aceitos em revistas indexadas (Qualis A2, B1 e B5), 2 publicações em anais de conferências nacionais organizadas pela Sociedade Brasileira de Computação (SBC), 3 publicações em *workshops* de especialistas e 6 publicações em conferências internacionais, sendo 4 destas de bastante destaque na área de Computação (Qualis A1/A2) e 2 delas de maior prestígio por serem diretamente organizadas pela Associação Internacional de Pesquisa em Criptologia (*International Association for Cryptologic Research – IACR*).

3.3. Biblioteca criptográfica

Um efeito colateral direto deste trabalho foi a fundação do projeto *RELIC* (*RELIC is an Efficient LIbrary for Cryptography*) [21]. O projeto teve como finalidade inicial a produção de uma biblioteca criptográfica para dispositivos embutidos que tivesse um menor consumo de memória que as alternativas. Atualmente, o projeto já constitui um *framework* completo para experimentação com implementação eficiente de algoritmos criptográficos, fornecendo ampla portabilidade e arquitetura modular especialmente projetada para permitir acelerações dependentes de arquitetura. A versão em repositório da biblioteca já atingiu a marca de 70 mil linhas de código, contando com mais de 8500 acessos de 1300 visitantes únicos provenientes de 74 países, e mais de 1500 *downloads* distribuídos nas 9 versões já disponibilizadas.

4. Conclusões

Dentre os vários recordes de velocidade para implementações em *software* no nível de segurança de 128 *bits* apresentados neste trabalho, nenhum foi superado até então. Desta forma, todos os resultados aqui apresentados permanecem como estado-da-arte em suas áreas correspondentes. São estes: recorde de velocidade para a multiplicação em curvas binárias genéricas resistente a canais laterais e para o cálculo serial ou paralelo de emparelhamentos bilineares nos cenários simétrico e assimétrico. Estas contribuições foram disponibilizadas na forma de uma biblioteca criptográfica para microcontroladores e máquinas multiprocessadas.

Referências

[1] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22:644–654, November 1976.

[2] N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of computation*, 48:203–9, 1987.

[3] V. Miller. Uses of Elliptic Curves in Cryptography. In H. C. Williams, editor, *CRYPTO 85*, volume 218 of *LNCS*, pages 417–426. Springer, 1985.

[4] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[5] D. F. Aranha, D. Câmara, J. López, L. B. Oliveira, and R. Dahab. Implementação eficiente de criptografia de curvas elípticas em sensores sem fio. In *SBSEG 2008*, pages 173–186.

[6] D. F. Aranha, J. López, L. B. Oliveira, and R. Dahab. Efficient implementation of elliptic curves on sensor nodes. In *CHiLE 2009*, 2009.

[7] D. F. Aranha, L. B. Oliveira, J. López, and R. Dahab. Efficient implementation of elliptic curve cryptography in wireless sensors. *Adv. Math. Comm.*, 4(2):169–187, 2010.

[8] D. F. Aranha, J. López, and D. Hankerson. Efficient Software Implementation of Binary Field Arithmetic Using Vector Instruction Sets. In *LATINCRYPT 2010*, volume 6212 of *LNCS*, pages 144–161, 2010.

[9] J. Taverne, A. Faz-Hernández, D. F. Aranha, F. Rodríguez-Henríquez, D. Hankerson, and J. López. Software implementation of binary elliptic curves: Impact of the carry-less multiplier on scalar multiplication. In *CHES 2011*, volume 6917 of *LNCS*, pages 108–123. Springer, 2011.

[10] J. Taverne, A. Faz-Hernández, D. F. Aranha, F. Rodríguez-Henríquez, D. Hankerson, and J. López. Speeding scalar multiplication over binary elliptic curves using the new carry-less multiplication instruction. *J. Cryptographic Engineering*, 1(3):187–199, 2011.

[11] D. F. Aranha, L. B. Oliveira, J. López, and R. Dahab. NanoPBC: implementing cryptographic pairings on an 8-bit platform. In *CHiLE 2009*, 2009.

[12] L. B. Oliveira, D. F. Aranha, C. P. L. Gouvêa, M. Scott, D. F. Câmara, J. López, and R. Dahab. TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks. *Computer Communications*, 4(2):169–187, 2011.

[13] L. B. Oliveira, A. Kansal, C. P. L. Gouvêa, D. F. Aranha, J. López, B. Priyantha, M. Goraczko, and F. Zhao. Secure-TWS: Authenticating Node to Multi-user Communication in Shared Sensor Networks. *The Computer Journal*, 2011. To appear.

[14] V. S. Miller. The Weil Pairing, and Its Efficient Calculation. *Journal of Cryptology*, 17(4):235–261, 2004.

[15] D. F. Aranha and J. López. Paralelização em software do Algoritmo de Miller. In *SBSEG 2009*, pages 27–40, 2009.

[16] D. F. Aranha, J. López, and D. Hankerson. High-Speed Parallel Software Implementation of the η_T Pairing. In *SPEED-CC 2009*, pages 73–88, 2009.

[17] D. F. Aranha, J. López, and D. Hankerson. High-Speed Parallel Software Implementation of the η_T Pairing. In *CT-RSA 2010*, volume 5985 of *LNCS*, pages 89–105. Springer, 2010.

[18] D. F. Aranha, J.-L. Beuchat, J. Detrey, and N. Estibals. Optimal eta pairing on supersingular genus-2 binary hyperelliptic curves. In O. Dunkelman, editor, *CT-RSA 2012*, volume 7178 of *LNCS*, pages 98–115. Springer, 2012.

[19] D. F. Aranha, K. Karabina, P. Longa, C. H. Gebotys, and J. López. Faster Explicit Formulas for Computing Pairings over Ordinary Curves. In *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 48–68. Springer, 2010.

[20] D. F. Aranha, A. Menezes, E. Knapp, and F. Rodríguez-Henríquez. Parallelizing the Weil and Tate Pairings. In *IMACC 2011*, volume 7089 of *LNCS*, pages 275–295, 2011.

[21] D. F. Aranha and C. P. L. Gouvêa. RELIC is an Efficient LIbrary for Cryptography. `http://code.google.com/p/relic-toolkit/`.