TRABALHO DE FORMATURA SUPERVISIONADO

BIBLIOTECA CRIPTOGRÁFICA BASEADA EM TRAÇOS

XTR

Diogo Haruki Kykuta

Orientador: Prof. Dr. Paulo S. L. M. Barreto (Poli-USP)

Trabalho de Formatura Supervisionado

Instituto de Matemática e Estatística, Universidade de São Paulo

INTRODUÇÃO

Em criptografia, vários protocolos tem sua segurança garantida pela dificuldade do Problema do Logaritmo Discreto em grupos multiplicativos. Em geral, quando tentamos utilizar grupos cuja operação é simples, dado um nível de segurança fixo, costumamos precisar de mais bits para representar cada elemento. Por outro lado, normalmente grupos que levam a uma menor exigência de bits por elemento costumam ter implementações complexas.

XTR (originalmente ECSTR - Efficient and Compact Subgroup Trace Representation) é uma maneira de evitar a representação de elementos do corpo base, lidando apenas com seus traços, pertencentes a um subcorpo mais simples. Isso é feito de forma a preservar a segurança. Assim, conseguimos um protocolo que não requer um número exagerado de bits para representar cada elemento e ainda lidamos com operações relativamente simples (a maior parte delas é simplesmente operações em corpos inteiros).

NOTAÇÕES

O corpo base desse trabalho é o Corpo de Galois de tamanho p^6, que será representado por $GF(p^6)$. O traço de um elemento x de $GF(p^6)$ será denotado por Tr(x), com Tr(x) pertencente a $GF(p^2)$.

PARÂMETROS

Queremos um número primo p e um número primo q tais que:

→ $p = 2 \pmod 3$

→ q divide $p^2 - p + 1$

p será usado para definir o tamanho do corpo base, e q o tamanho do subgrupo multiplicativo escolhido.

Para obtermos a segurança de 1024 bits, precisamos que p tenha aproximadamente 1024/6 bits, ou seja 170 bits. Assim, representar um elemento de $GF(p^2)$ utiliza cerca de 340 bits.

ESCOLHA DO SUBGRUPO

Queremos um elemento g de $GF(p^6)$ que tenha ordem q. Como elementos desse corpo nunca são representados, basta encontrarmos algum Tr(g) tal que $|g| = q$. A biblioteca fornece um método que encontra um tal Tr(g).

OPERAÇÕES

EXPONENCIAÇÃO SIMPLES

Como evitamos a representação de elementos de $GF(p^6)$, devemos conseguir realizar exponenciações conhecendo apenas seu traço. Um método para isso é descrito por Lenstra e Verheul [1] e foi implementado na biblioteca. Conhecendo os corpos sobre os quais estamos trabalhando, Tr(g) e um inteiro n, conseguimos calcular $Tr(g^n)$.

EXPONENCIAÇÃO DUPLA

Chamamos assim quando queremos calcular, por exemplo, $Tr(g^a * g^{bk})$, não conhecendo k, somente $Tr(g^k)$. O método descrito no artigo requer duas informações extras: $Tr(g^{k-1})$ e $Tr(g^{k+1})$. Por requerer essas informações a mais, os autores provaram que seu conhecimento público delas não prejudica a segurança dos protocolos.

CHAVES

Existe na biblioteca uma definição genérica e padrão de um par de chaves pública / privada. Esse par de chaves pode ser utilizado por qualquer versão XTR dos protocolos criptográficos.

VERSÕES XTR DE ALGUNS PROTOCOLOS

Para testar a biblioteca, as versões XTR da Criptografia ElGamal e da Assinatura Schnorr foram implementadas. Com elas, conseguimos cobrir exemplos de utilização da exponenciação simples e dupla.

Qualquer protocolo que utilize apenas exponenciações simples ou dupla podem ter suas versões XTR implementados com o auxílio dessa biblioteca.

CONCLUSÕES

Com a construção dessa biblioteca, conseguimos ver que implementar as operações foi relativamente fácil, por serem basicamente operações em números inteiros.

Apesar de funcional, a biblioteca ainda não está enxuta. Existem muitas otimizações possíveis, o que pode prover notória diferença no espaço requerido para armazenar a biblioteca. Assim, talvez seja possível sua utilização em ambientes onde a criptografia, em níveis de segurança adequados, era considerada inviável por insuficiência computacional, por exemplo sistemas embarcados.

REFERÊNCIA

[1] Arjen K. Lenstra e Eric R. Verheul. The xtr public key system. Em CRYPTO'00, páginas 1-19, 2000.