Biblioteca Criptográfica baseada em Traços XTR

Diogo Haruki Kykuta

Orientação

Prof. Dr. Paulo S. L. M. Barreto

Poli

Introdução

Objetivos

- Biblioteca compacta
- Número reduzido de bits para representar cada elemento

Só para relembrar...
Corpo de Galois = Corpos Finitos

$GF(p^t)$
é um corpo com p^t elementos; onde p é um primo e $t \in \mathbb{Z}$

O que é XTR?

Mas... O que é XTR?

O que é XTR?

ECSTR: Efficient and Compact Subgroup Trace Representation

O que é XTR?

ECSTR: Efficient and Compact Subgroup Trace Representation

Ao invés de representarmos um elemento de $GF(p^6)$, usamos seu traço, que é um elemento de $GF(p^2)$

- Menos bits por elemento
- Operações mais simples

O que é XTR?

Onde usar XTR?

O que é XTR?

Onde usar XTR?
Qualquer protocolo que seja baseado no uso de subgrupos

- Diffie-Hellman
- ElGamal
- Assinatura Schnorr
- Muitos outros...

Problema do Logaritmo Discreto

Em um corpo conhecido...
Conhecendo g, g^a é difícil descobrir a

XTR

Parâmetros XTR

Parâmetros XTR

- p primo

Parâmetros XTR

- p primo
- q primo

Parâmetros XTR

- p primo
- q primo
- com q dividindo $p^2 - p + 1$

Biblioteca XTR

- **Geração dos parâmetros**

Escolha do subgrupo

Elemento g de $GF(p^6)$

Escolha do subgrupo

Elemento g de $GF(p^6)$

Onde a ordem de g é q
$|g| = q$

Escolha do subgrupo

Elemento g de $GF(p^6)$

Onde a ordem de g é q
$|g| = q$

$Tr(g) \in GF(p^2)$

Biblioteca XTR

- Geração dos parâmetros
- **Encontrar** $Tr(g)$ **com** $|g| = q$

Chaves

Chaves convencionais
Informações públicas: p, q, g, g^k
Informação privada: k

Chaves

Chaves convencionais
Informações públicas: p, q, g, g^k
Informação privada: k

Chaves XTR
Informações públicas: $p, q, Tr(g), Tr(g^k)$
Informação privada: k

Biblioteca XTR

- Geração dos parâmetros
- Encontrar $Tr(g)$ com $|g| = q$
- **Geração de um par de chaves**

$Tr(g^k)$?

Repare que não podemos garantir que
$Tr(g)^k = Tr(g^k)$

Biblioteca XTR

- Geração dos parâmetros
- Encontrar $Tr(g)$ com $|g| = q$
- Geração de um par de chaves
- **Permitir a exponenciação simples**
  Ou seja, dado $Tr(g)$ e n, calcular $Tr(g^n)$

Com isso, já é possível implementar, por exemplo, criptografia ElGamal.

Mas... E Assinatura Schnorr?
É possível implementá-la?

Mas... E Assinatura Schnorr?
É possível implementá-la? Não.

Mas... E Assinatura Schnorr?
É possível implementá-la? Não. Ainda não.

$y = g^k$, com k desconhecido

$y = g^k$, com k desconhecido
$s \in \mathbb{Z}$
$e \in \mathbb{Z}$

$y = g^k$, com k desconhecido
$s \in \mathbb{Z}$
$e \in \mathbb{Z}$
Calcular $g^s y^e = g^s g^{ke}$.

No caso do XTR, seria equivalente a calcular $Tr(g^s * g^{ke})$ conhecendo-se $Tr(g), Tr(g^k), s, e$.

Biblioteca XTR

- Geração dos parâmetros
- Encontrar $Tr(g)$ com $|g| = q$
- Geração de um par de chaves
- Permitir a exponenciação simples
  Ou seja, dado $Tr(g)$ e n, calcular $Tr(g^n)$
- **Permitir a exponenciação dupla**
  Ou seja, dados $Tr(g)$, $Tr(g^k)$, a, b, calcular $Tr(g^a * g^{kb})$

No artigo, há um método para se calcular essa exponenciação dupla, mas são necessárias mais informações.

No artigo, há um método para se calcular essa exponenciação dupla, mas são necessárias mais informações.

Precisamos de $Tr(g^{k-1})$ e $Tr(g^{k+1})$.

Biblioteca XTR

- Geração dos parâmetros
- Encontrar $Tr(g)$ com $|g| = q$
- Geração de um par de chaves
- Permitir a exponenciação simples
  Ou seja, dados $Tr(g)$ e n, calcular $Tr(g^n)$
- Permitir a exponenciação dupla
  Ou seja, dados $Tr(g)$, $Tr(g^{k-1})$, $Tr(g)$, $Tr(g^{k+1})$, a, b,
  calcular $Tr(g^a * g^{kb})$

Mas...

Mas... Não temos essas informações na chave pública...

Chaves

Chaves XTR antes
Informações públicas: $p, q, Tr(g), Tr(g^k)$
Informação privada: k

Chaves

Chaves XTR antes
Informações públicas: $p, q, Tr(g), Tr(g^k)$
Informação privada: k

Chaves XTR depois
Informações públicas: $p, q, Tr(g), Tr(g^{k-1}), Tr(g^k), Tr(g^{k+1})$
Informação privada: k

Essas informações a mais não prejudicam a segurança

Essas informações a mais não prejudicam a segurança

Agora sim, conseguimos prover tudo que é necessário para implementarmos uma assinatura Schnorr.

Biblioteca pronta.
Temos uma biblioteca que supre todas as necessidades encontradas para implementar os diversos protocolos baseados em escolha de subgrupos.

Próximos Passos

- Otimizar a biblioteca
- Torná-la enxuta

Obrigado