



Universidade
Federal do Pará



Uma Proposta de Integração da Biblioteca Criptográfica do Sistema Helios ao Sistema Civis

Paula Santos e Roberto Samarone Araujo

Setembro/2024

XVIII Workshop de Trabalhos de Iniciação Científica e de Graduação (WTICG)

AGENDA

- ✓ Introdução
- ✓ Motivação
- ✓ Contribuição
- ✓ Os sistemas votação Helios e Civis
- ✓ Proposta de Integração
- ✓ Conclusão e Trabalhos Futuros

INTRODUÇÃO



- ✓ Digitalização de serviços (Covid-19)
- ✓ Eleições via Internet
 - Reitores em universidades
- ✓ Sistemas de votação
 - presencial – Online
- ✓ Sistemas seguros
 - Helios
 - Civis

MOTIVAÇÃO

✓ O Sistema Helios

- Verificação Fim-a-Fim
 - Mecanismos criptográficos
- Criptosistema ElGamal



- Literatura apresenta vários estudos
- Biblioteca amplamente testada e validada em cenários reais

✓ O Sistema Civis

- Resistência à coerção
 - Mecanismos criptográficos
- Criptosistema ElGamal

É POSSÍVEL INTEGRAR A BIBLIOTECA CRIPTOGRÁFICA UTILIZADA NO SISTEMA HELIOS AO SISTEMA CIVIS ?

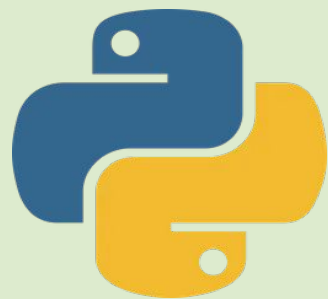
CONTRIBUIÇÃO

Uma Proposta de Integração do Criptosistema ElGamal do Sistema Helios ao Sistema Civis

Os Sistemas de Votação Helios e Civis

O Sistema HELIOS

TECNOLOGIAS



Arquitetura

Cliente/Servidor

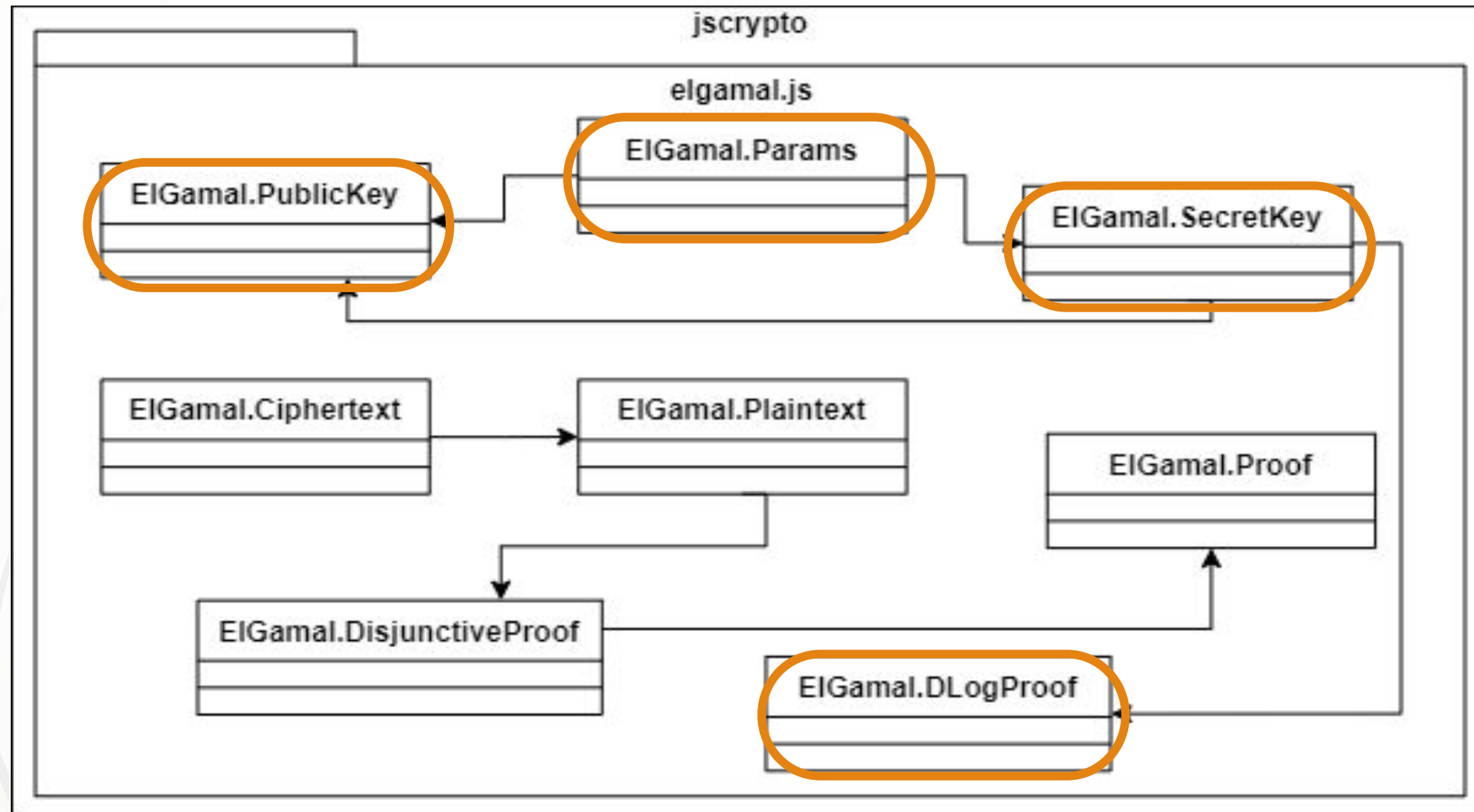
PRIMITIVAS CRIPTOGRÁFICAS

- Criptosistema ElGamal
- Provas de conhecimento (NIZKPs)

Os Sistemas de Votação Helios e Civis

O Sistema HELIOS

Classes (Cliente)



Simplificado

Estrutura Funcional - Eleição

1. Configuração

- Elgamal.Params
- ElGamal.PublicKey
- ElGamal.SecretKey
- ElGamal.DlogProof

Parâmetros fixos

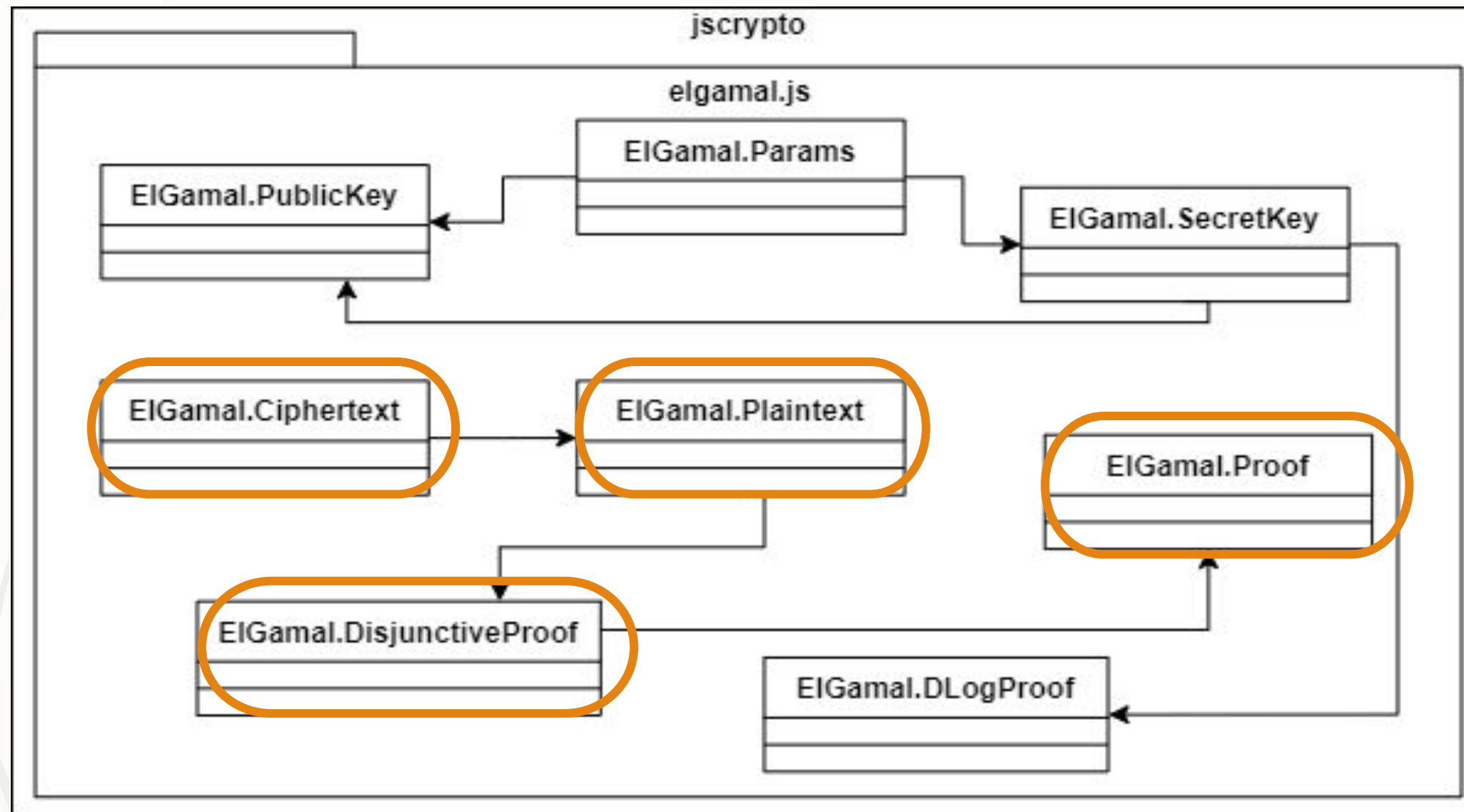
Primos: p, q

Gerador: g

Os Sistemas de Votação Helios e Civis

O Sistema HELIOS

Classes (Cliente)



Simplificado

Estrutura Funcional - Eleição

1. Configuração

- EIGamal.Params
- EIGamal.PublicKey
- EIGamal.SecretKey
- EIGamal.DlogProof

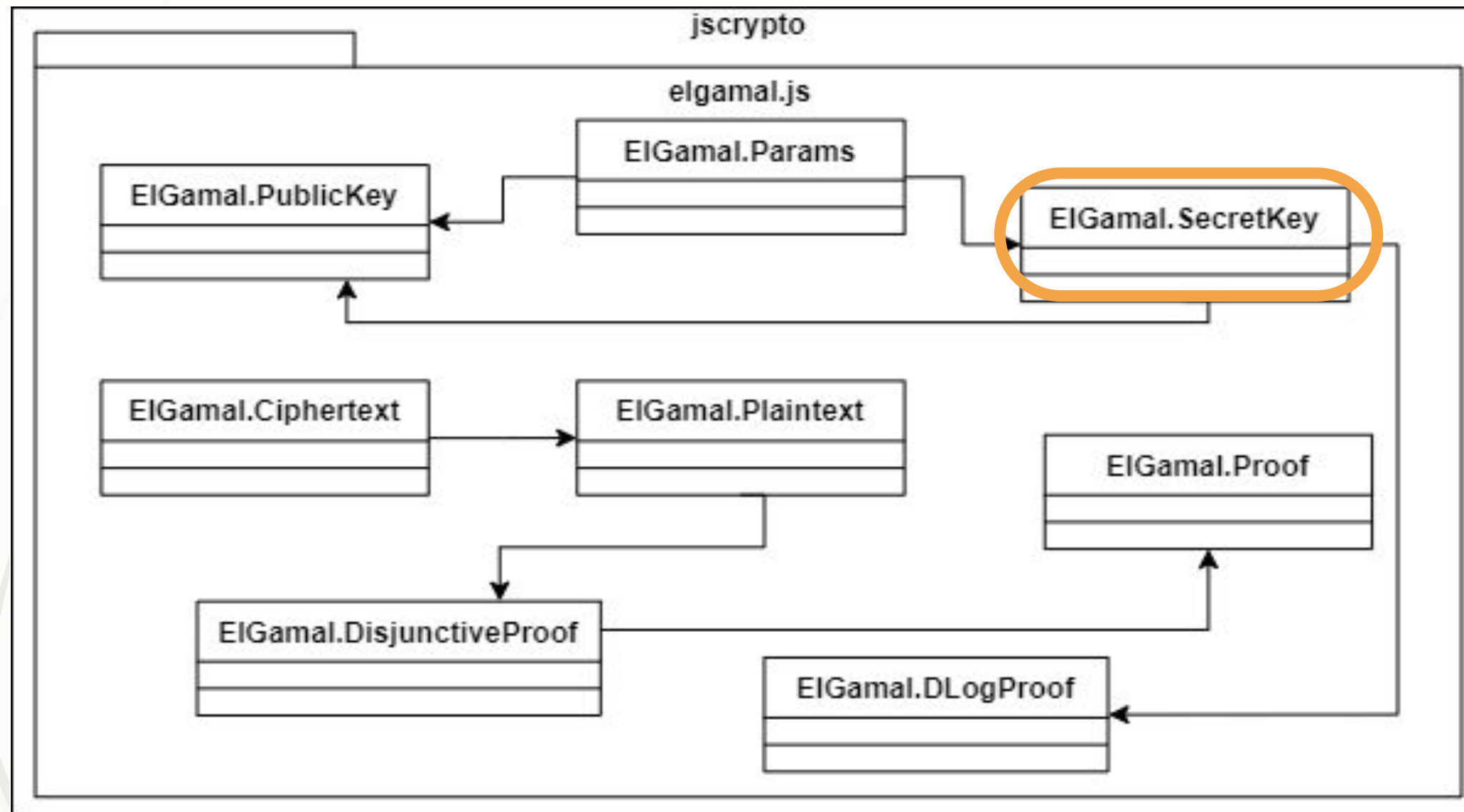
2. Votação

- EIGamal.Plaintext
- EIGamal.Ciphertext
- EIGamal.Proof
- EIGamal.DisjunctiveProof

Os Sistemas de Votação Helios e Civis

O Sistema HELIOS

Classes (Cliente)



Simplificado

Estrutura Funcional - Eleição

1. Configuração

- ElGamal.Params
- EIGamal.PublicKey
- EIGamal.SecretKey
- EIGamal.DlogProof

2. Votação

- EIGamal.Plaintext
- EIGamal.Ciphertext
- EIGamal.Proof
- EIGamal.DisjunctiveProof

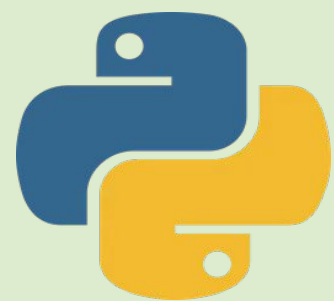
3. Apuração

- EIGamal.SecretKey
decryptAndProve e
decrypt

Os Sistemas de Votação Helios e Civis

O Sistema CIVIS

TECNOLOGIAS



Arquitetura

Cliente/Servidor

PRIMITIVAS CRIPTOGRÁFICAS

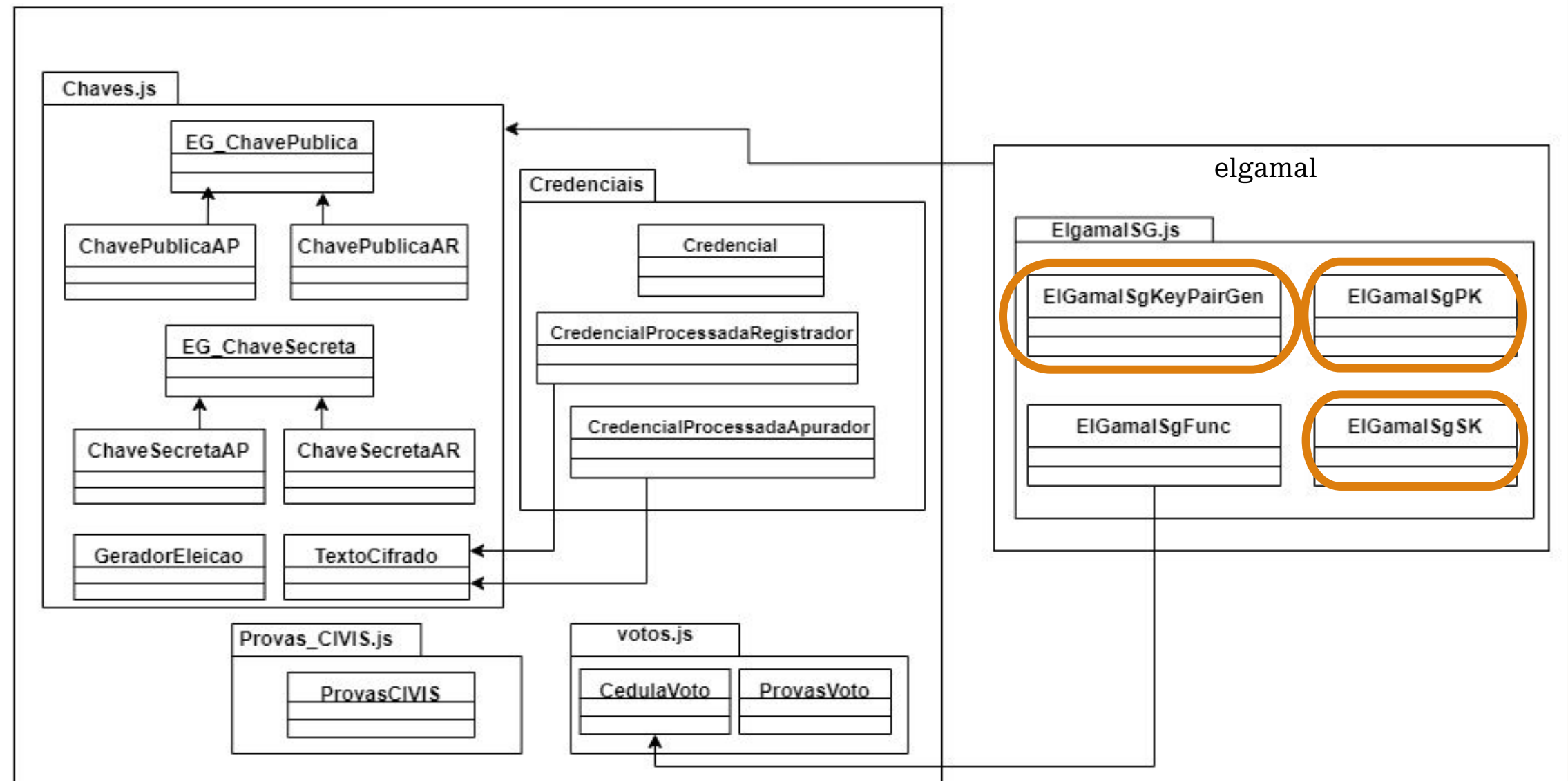
- Criptosistema ElGamal
- Provas de conhecimento (NIZKPs)
- Rede de Misturadores

Os Sistemas de Votação Helios e Civis

O Sistema CIVIS

Classes (cliente)

Estrutura Funcional - Eleição



Simplificado

1. Configuração

- Elgama1SgKeyPairGen
- ElGama1SgPK
- ElGama1SgSK

Parâmetros gerados dinamicamente

Primos: p, q

Gerador: g

Os Sistemas de Votação Helios e Civis

O Sistema CIVIS

Classes (cliente)

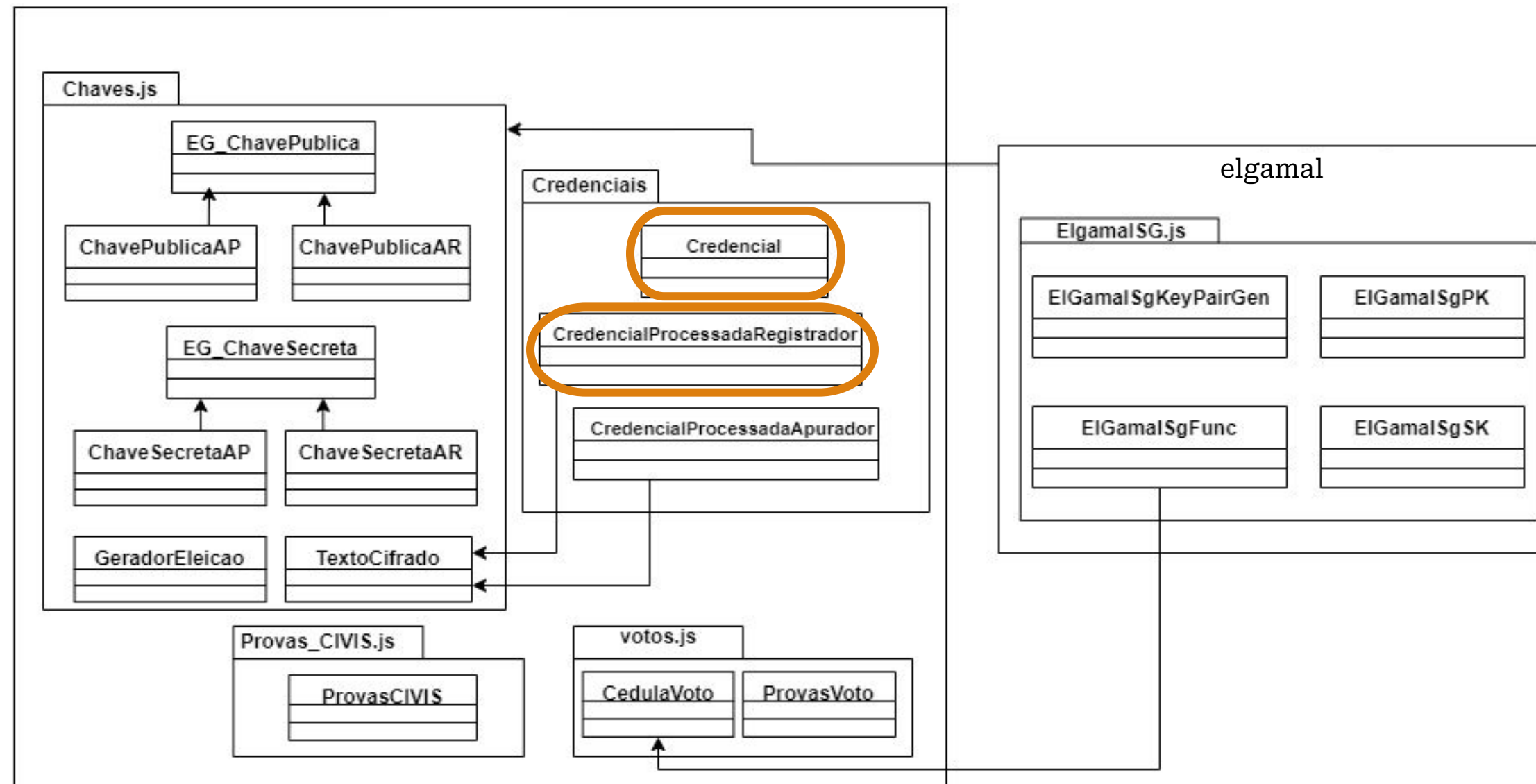
Estrutura Funcional - Eleição

1. Configuração

- ElgamaISgKeyPairGen
- ElGamaISgPK
- ElGamaISgSK

2. Registro

- Credencial
- CredencialProcessadaRegistrador



Simplificado

Os Sistemas de Votação Helios e Civis

O Sistema CIVIS

Classes (cliente)

Estrutura Funcional - Eleição

1. Configuração

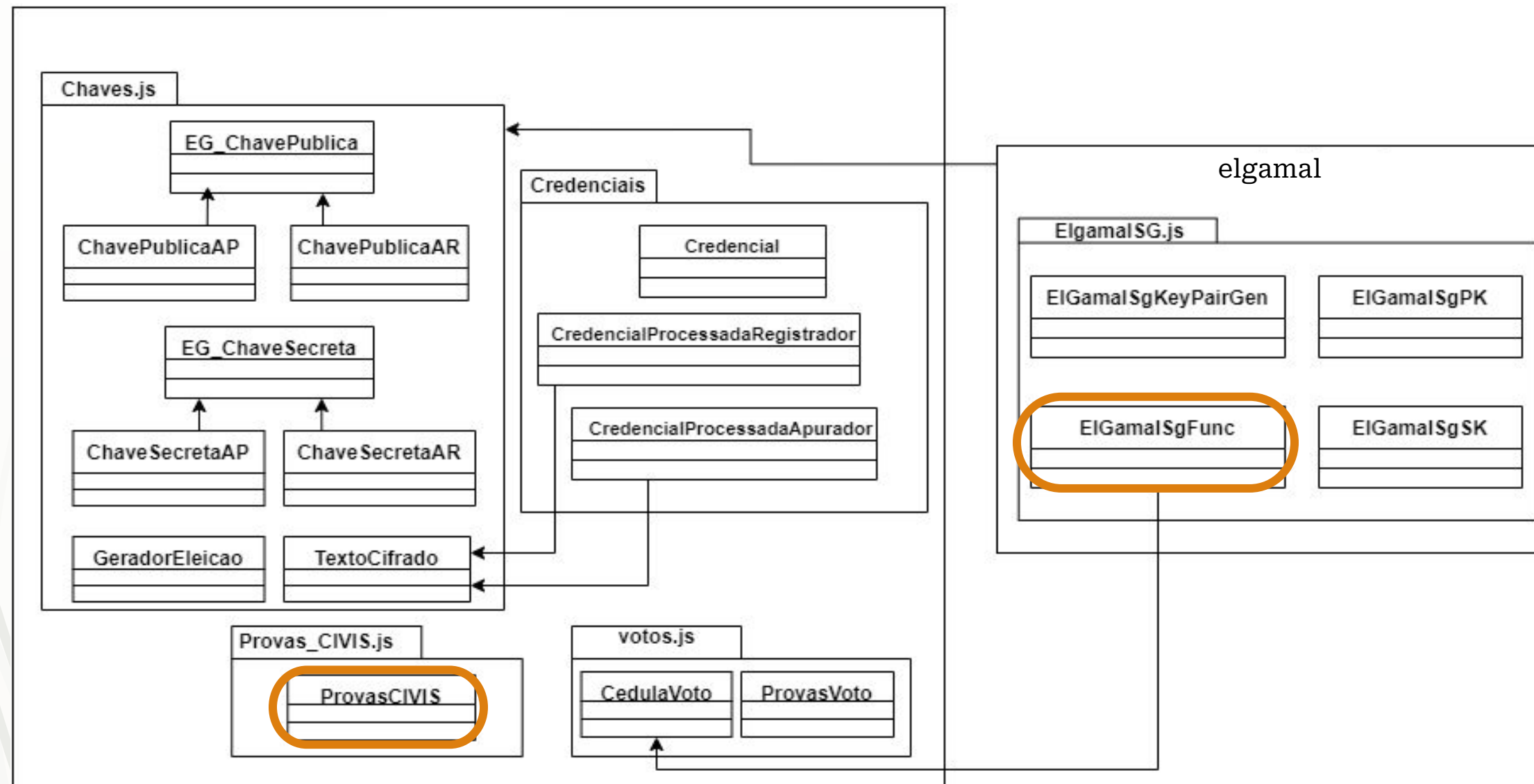
- ElGamalSgKeyPairGen
- ElGamalSgPK
- ElGamalSgSK

2. Registro

- Credencial
- CredencialProcessadaRegistrador

3. Votação

- ElGamalSgFunc
- ProvasCivis

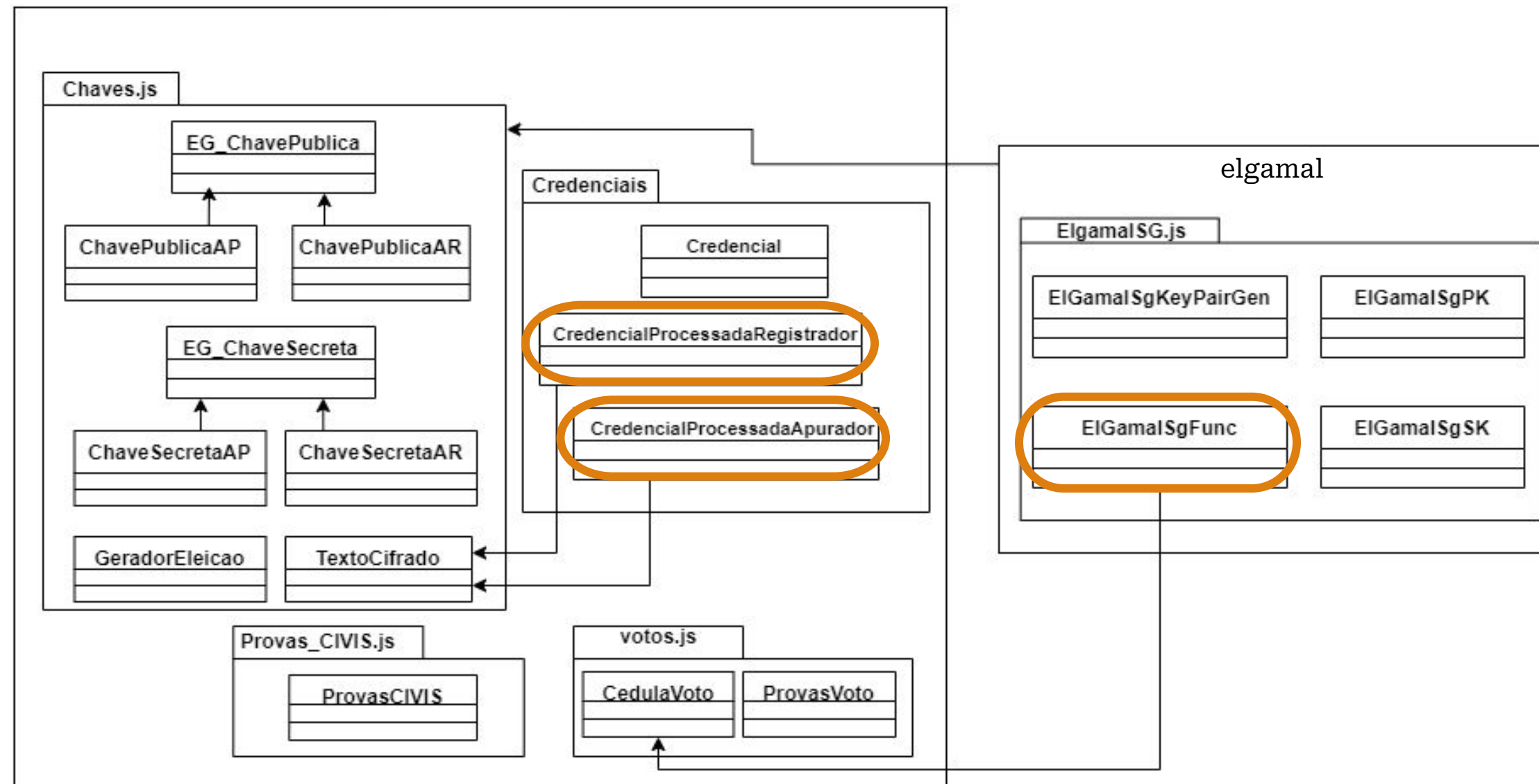


Simplificado

Os Sistemas de Votação Helios e Civis

O Sistema CIVIS

Classes (cliente)



Simplificado

Estrutura Funcional - Eleição

1. Configuração

- ElgamaISGKeyPairGen
- ElGamaISGPK
- ElGamaISGSK

2. Registro

- Credencial
- CredencialProcessadaRegistrador

3. Votação

- ElGamaISGFunc
- ProvasCivis

4. Apuração

- CredencialProcessadaRegistrador
- CredencialProcessadaApurador
- ElGamaISGFunc



PROPOSTA DE INTEGRAÇÃO

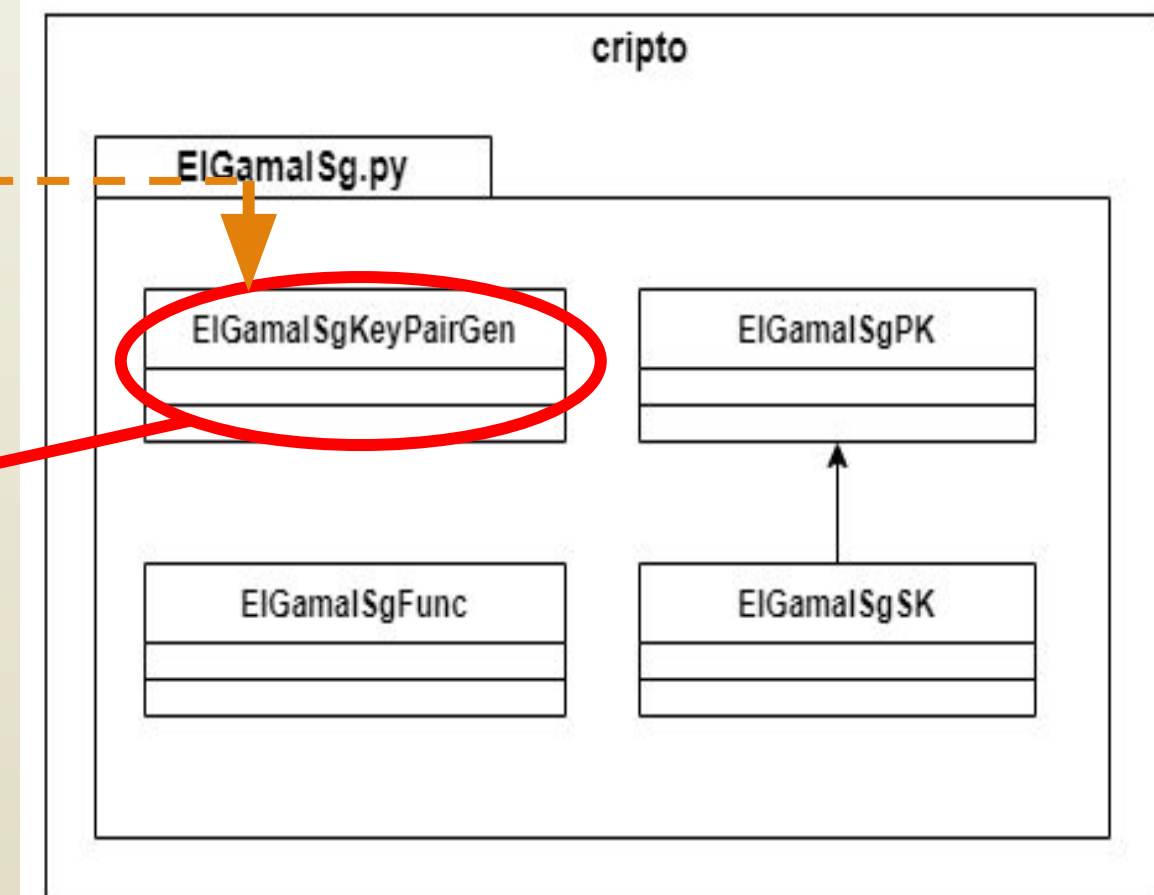
PROPOSTA DE INTEGRAÇÃO

ElGamal (Helios) -> Civis

Classes Civis (Servidor)

- Parâmetros Fixos
 - Grupo numérico: p, q
 - Geradores: g
 g_1, g_3 e o

Classes (servidor)

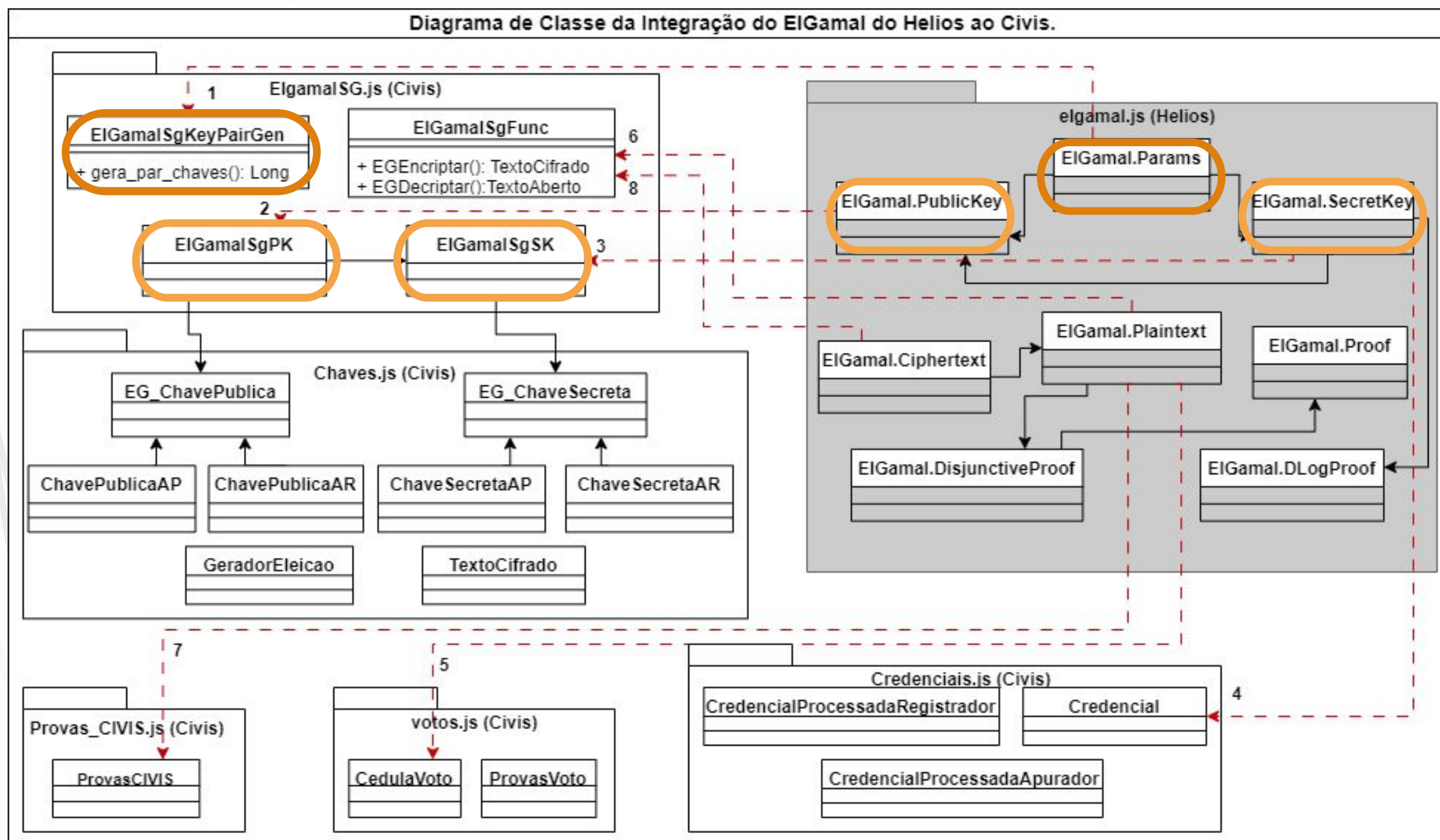


Helios

Civis

PROPOSTA DE INTEGRAÇÃO

Classes Civis (Cliente)



1ª Alteração - Geração

(Helios) → (Civis)

`ElGamal.Params` - Generate

→ `ElGamalSgKeyPairGen` - `Gera_par_chaves`

2ª e 3ª Alterações - Codificação

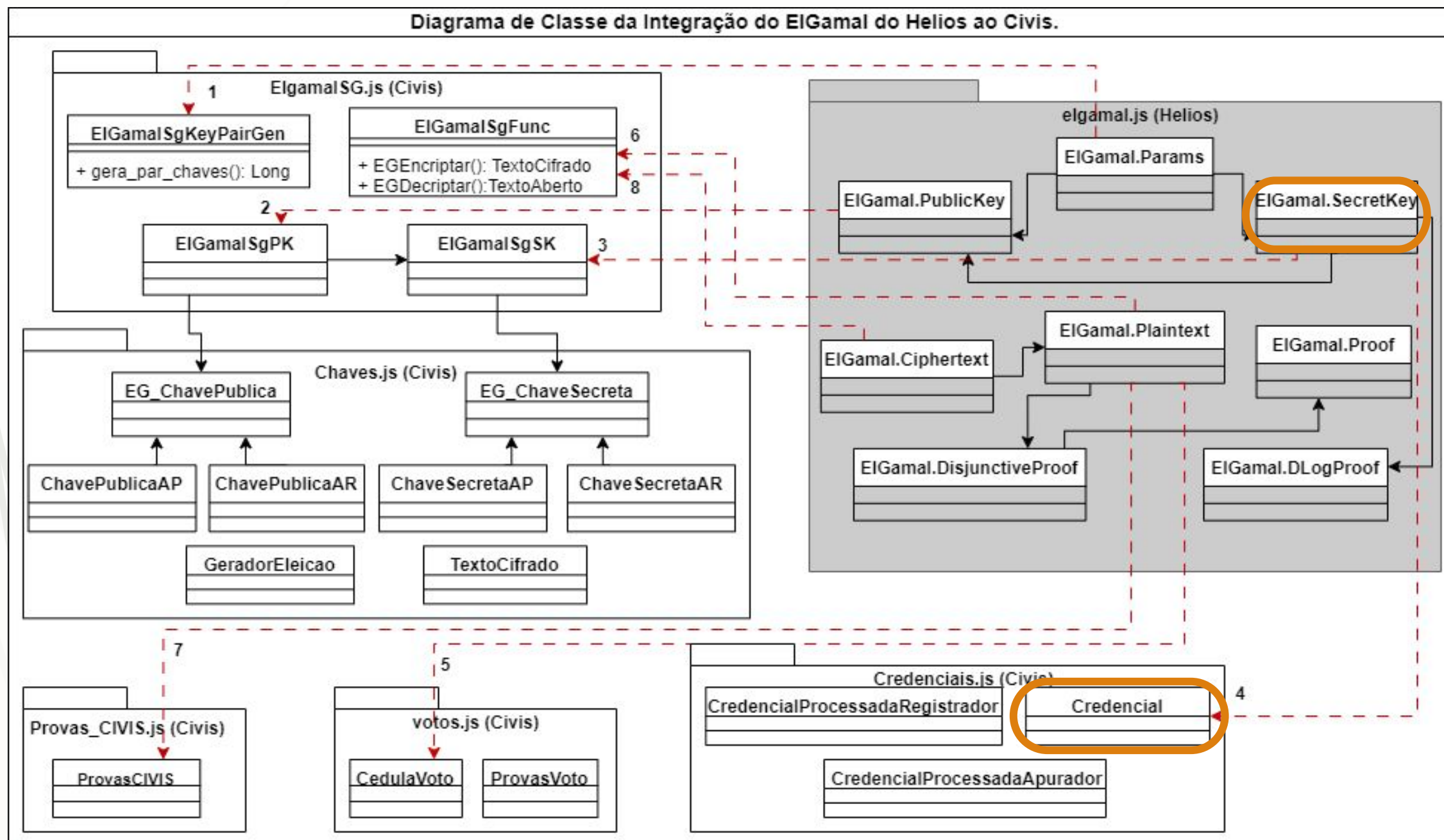
(Helios) → (Civis)

`ElGamal.SecretKey` e `ElGamal.PublicKey`

→ `ElGamalSgPK` e `ElGamalSgSK`

PROPOSTA DE INTEGRAÇÃO

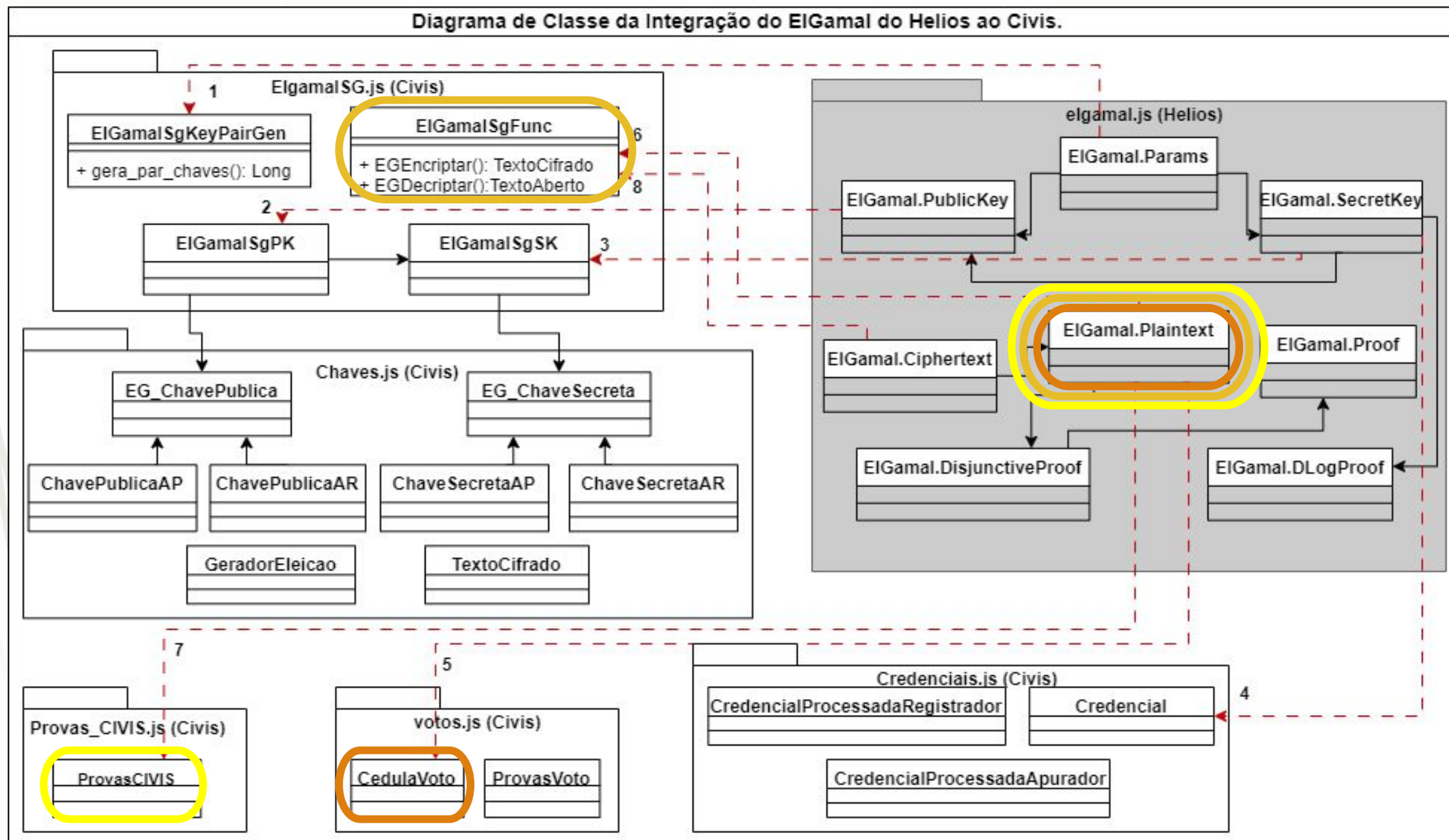
Classes Civis (Cliente)



4° Alteração - Credencial
(Helios) → (Civis)
ElGamal.Secretkey → Credenciais

PROPOSTA DE INTEGRAÇÃO

Classes Civis (Cliente)



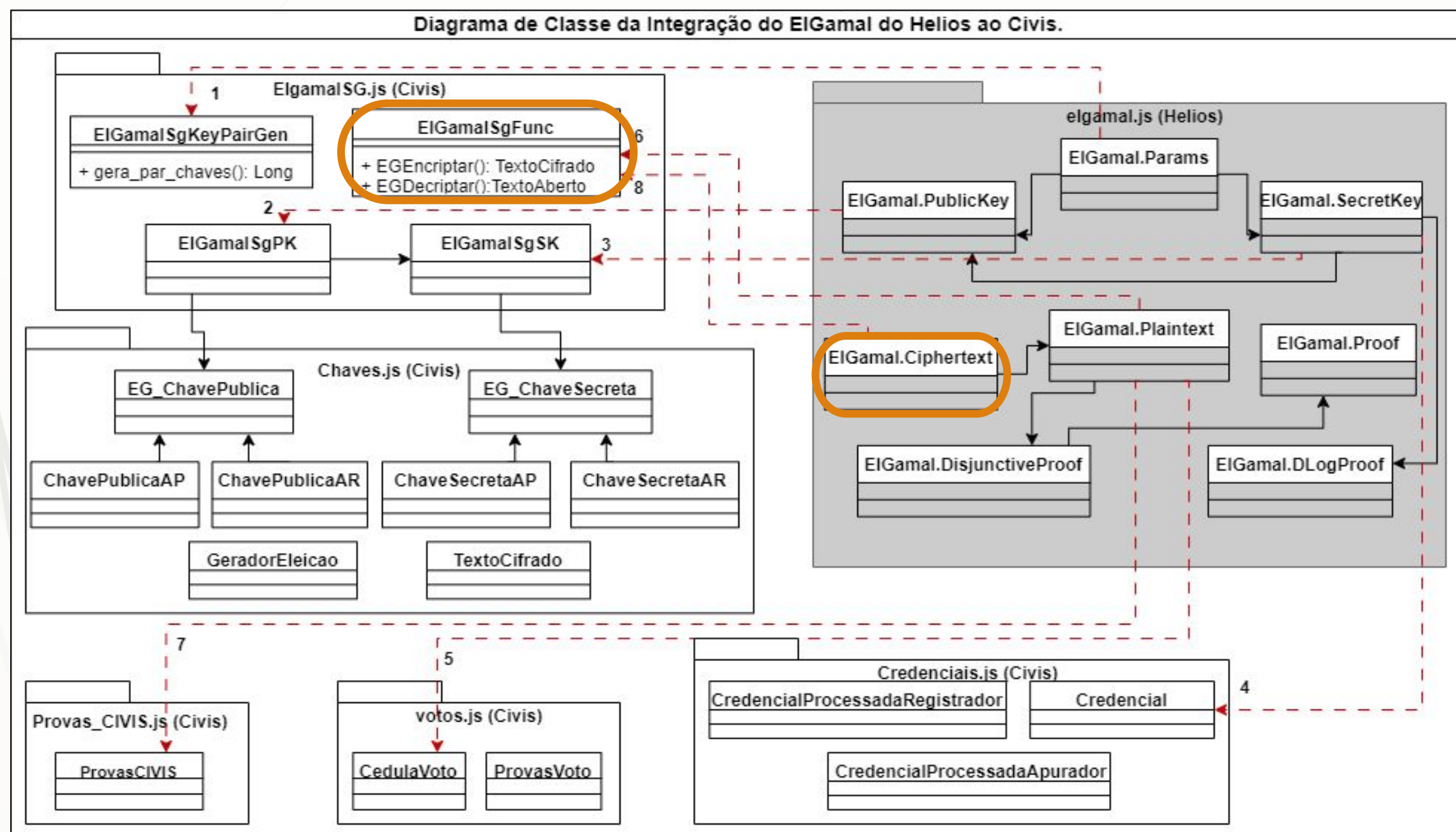
5° Alteração - Tratamento dos votos
(Helios) → (Civis)
ElGamal.Plaintext → *CedulaVoto*

6° Alteração - Encriptação
(Helios) → (Civis)
ElGamal.Plaintext - encrypt
→ *ElGamalSgFunc* - *EGENcriptar*

7° Alteração - NIZKP
(Helios) → (Civis)
ElGamal.Plaintext
→ *ProvasCivis* - *gerarPValidVotoEnc*





PROPOSTA DE INTEGRAÇÃO

Classes Civis (Cliente)



8° Alteração - Decifração
(Helios) → (Civis)
`EIGamal.Ciphertext`
→ `EIGamalSgFunc - EGDecryptar`

CONCLUSÃO E TRABALHOS FUTUROS

-  Este trabalho apresentou uma proposta de integração da biblioteca criptográfica utilizada pelo sistema Helios ao sistema Cavis.
-  A integração responde parcialmente o questionamento proposto anteriormente, pois foi integrado apenas o criptosistema ElGamal.
-  Outras primitivas criptográficas presentes na biblioteca do sistema Helios são deixados como trabalhos futuros.
-  Avaliações empíricas de estudos de casos em ambientes reais de votação são deixados como trabalhos futuros.

Muito Obrigada



Belém-Pará