Um estudo sobre
conceitos criptográficos
aplicáveis em compartilhamento de informações em
rede social
com provedor de serviço não confiável

Adriano dos Reis Lopes
Orientador Prof. Dr. Paulo S. L. M. Barreto
Trabalho de formatura supervisionado
DCC IME USP

Motivação

- Alcance das redes sociais online

Motivação

- Alcance das redes sociais online
- Premissas do mundo virtual ≠ real

Motivação

- Alcance das redes sociais online
- Premissas do mundo virtual ≠ real
- Criptografia provê privacidade

Por que um provedor de serviço não confiável?

- Nuvem não é um meio confiável

Por que um provedor de serviço não confiável?

- Nuvem não é um meio confiável
- “JP Morgan descobre violação de dados por hackers” (noticia publicada em 3 de novembro de 2014 na reuters)

Por que um provedor de serviço não confiável?

- Nuvem não é um meio confiável
- “JP Morgan descobre violação de dados por hackers” (noticia publicada em 3 de novembro de 2014 na reuters)
- Snowden

OK, mas por onde começar?

Há alguma rede social assim?

- Diáspora*
  - Rede federada: você pode adicionar seu próprio servidor.

Há alguma rede social assim?

- Diáspora*
  - Rede federada: você pode adicionar seu próprio servidor.
  - Comunicação criptografada

Há alguma rede social assim?

- Diáspora*
  - Rede federada: você pode adicionar seu próprio servidor.
  - Comunicação criptografada
  - Os servidores não necessariamente armazenam informações de modo criptografado

Casos de uso de rede social

- *Facebook*

Casos de uso de rede social

- *Facebook*

- Problemas mapeados:
  - Informações para contato (só interno à rede)

Casos de uso de rede social

- *Facebook*

- Problemas mapeados:
  - Informações para contato (só interno à rede)
  - Conversas (individuais e em grupo)

Casos de uso de rede social

- *Facebook*

- Problemas mapeados:
  - Informações para contato (só interno à rede)
  - Conversas (individuais e em grupo)
  - Publicações (Pessoais e em páginas)

Criptografia

- Secure Broadcasting with secure lock

Criptografia

- Secure Broadcasting with secure lock

- Conversa fora de registro multi usuário (MPOTR, na siglas em inglês)

Criptografia

- Secure Broadcasting with secure lock
- Conversa fora de registro multi usuário (MPOTR, na siglas em inglês)
- Criptografia baseada em atributos (ABE, na sigla em inglês)

Criptografia clássica

- Basta cada um enviar cada mensagem, cada informação a cada amigo de modo criptografado!

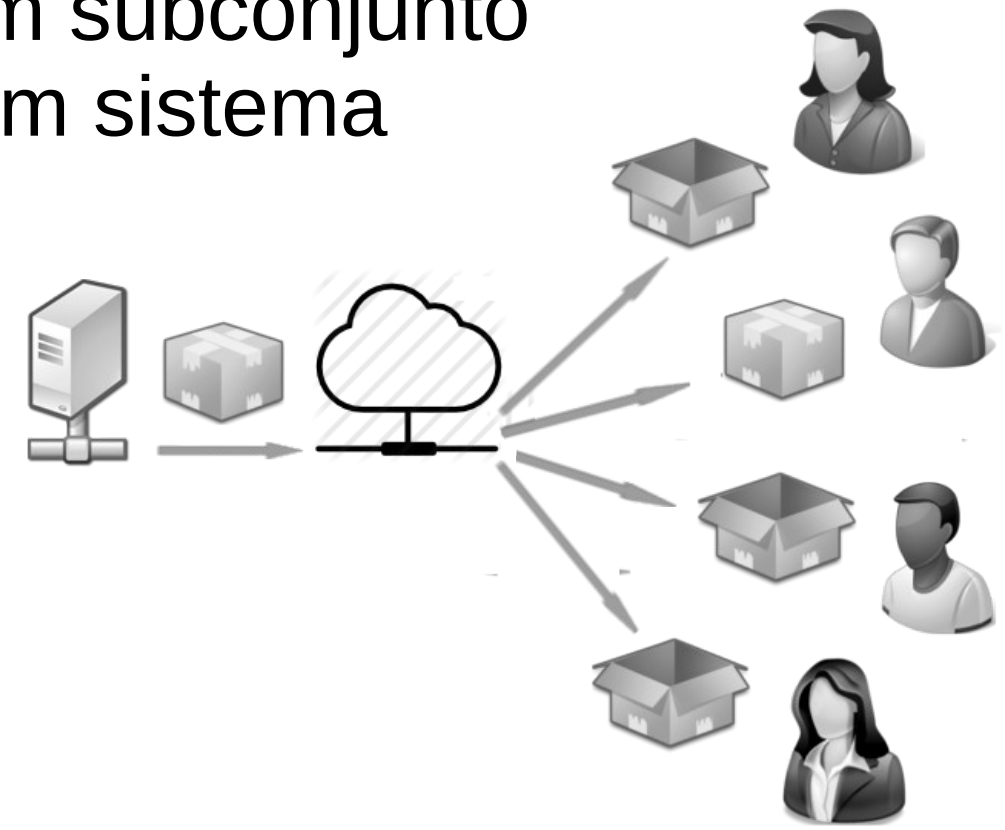
Criptografia clássica insuficiente

- Basta cada um enviar cada mensagem, cada informação a cada amigo de modo criptografado!

- Necessita de repetição: uma mesma mensagem é criptografada para cada um.

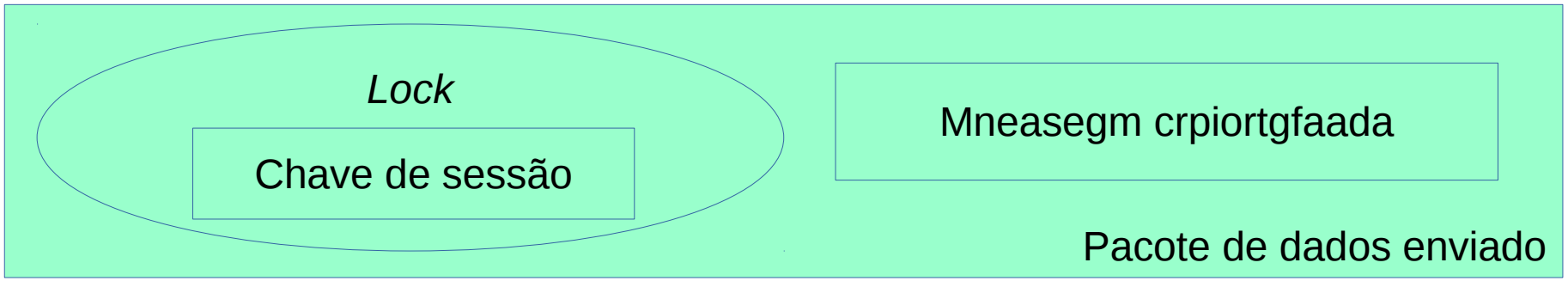
Criptografia de *broadcast*: um inicio

Um modo de mandar uma mensagem a um subconjunto de usuário de um sistema



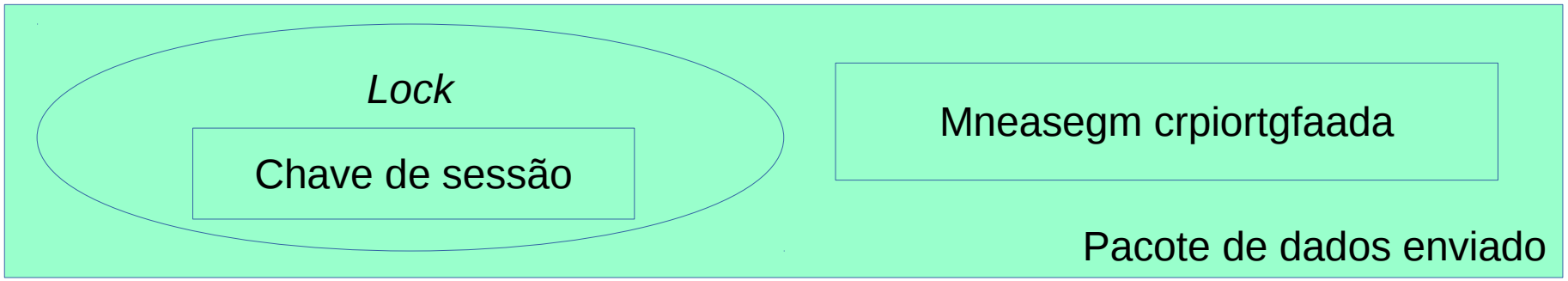
Criptografia de *broadcast*: uma solução (?)

- *Secure broadcasting with secure lock*
  - Usa números primos grandes e o Teorema Chinês do Resto
  - Criptografa a mensagem com a chave de sessão e guarda a chave dentro do lock, que só pode ser aberta por um subconjunto de usuários



Criptografia de *broadcast*: uma solução (?)

- *Secure broadcasting with secure lock*
  - Usa números primos grandes e o Teorema Chinês do Resto
  - Criptografa a mensagem com a chave de sessão e guarda a chave dentro do lock, que só pode ser aberta por um subconjunto de usuários



- Problema: depende de um servidor central que precisa conhecer todas as chaves de usuários

MPOTR Messaging: uma solução parcial

- Protocolo pensado na implementação

MPOTR Messaging: uma solução parcial

- Protocolo pensado na implementação

- Cria chave de sessão em uma comunicação inicial com autenticação e a usa para manter a conversa.

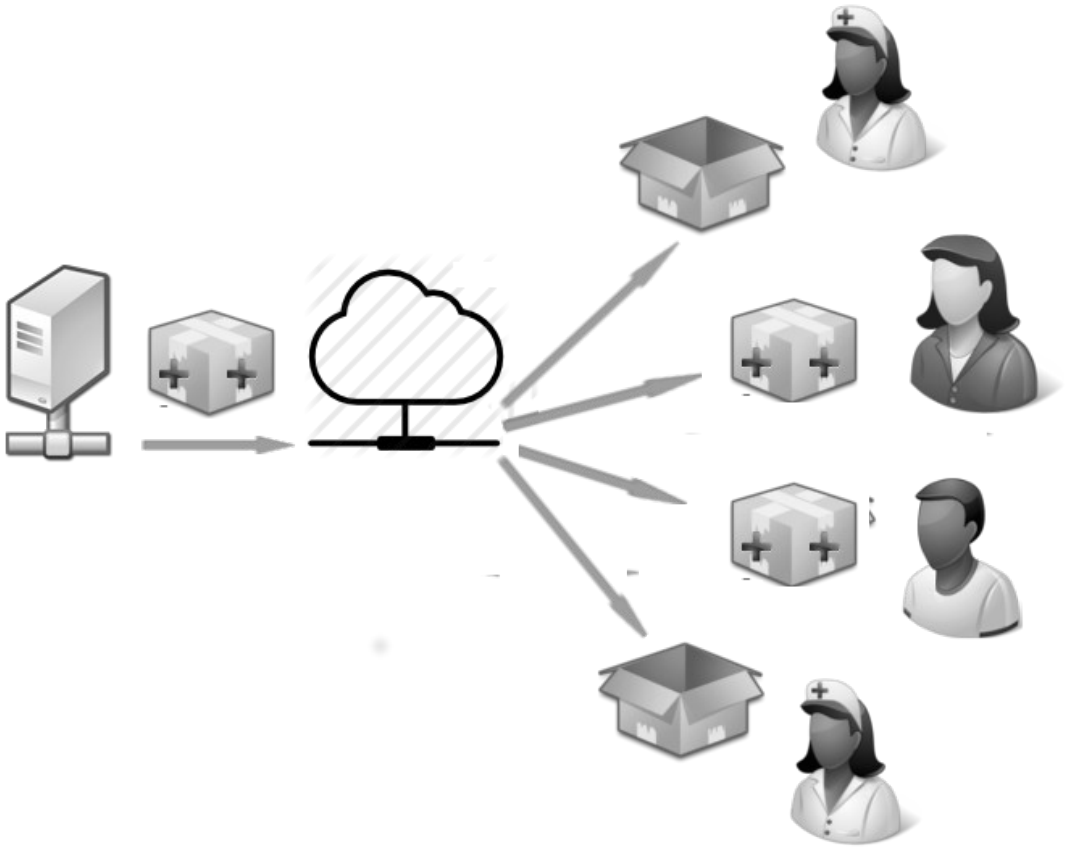
MPOTR Messaging: uma solução parcial

- Protocolo pensado na implementação
- Cria chave de sessão em uma comunicação inicial com autenticação e a usa para manter a conversa.
- Soluciona o problema para as conversas. Não depende da confiança no servidor da aplicação

MPOTR Messaging: uma solução parcial

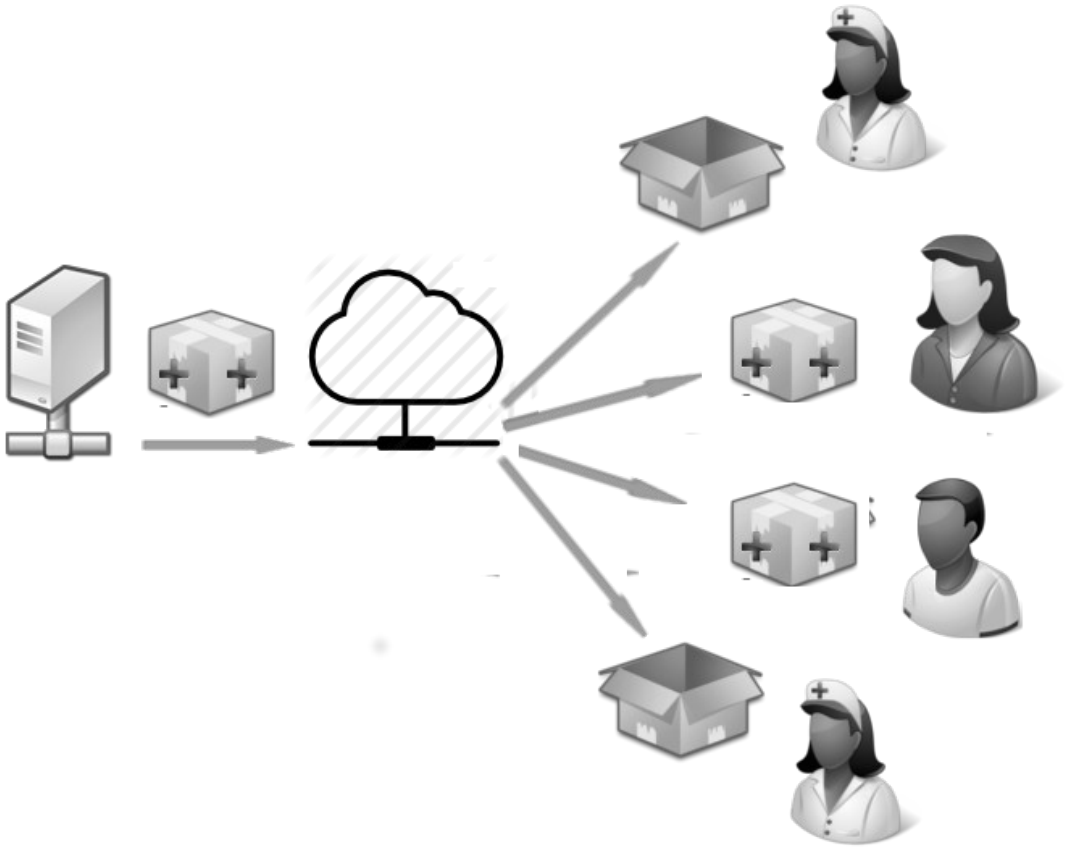
- Protocolo pensado na implementação
- Cria chave de sessão em uma comunicação inicial com autenticação e a usa para manter a conversa.
- Soluciona o problema para as conversas. Não depende da confiança no servidor da aplicação
- Não é adaptado e eficaz para os demais casos de uso.

ABE



- Origem:
  - Criptografia baseada em identidade

ABE



- Origem:
  - Criptografia baseada em identidade
- Ideia:
  - Atributos devem definir quem pode ou não decriptografar as informações

ABE

- Continua em desenvolvimento:
  - Matemático: ainda sem implementação

ABE

- Continua em desenvolvimento:
  - Matemático: ainda sem implementação
- Necessidade de servidores centrais
  - Tanto para criptografar os dados e para prover os atributos à cada usuário

ABE

- Continua em desenvolvimento:
  - Matemático: ainda sem implementação
- Necessidade de servidores centrais
  - Tanto para criptografar os dados e para prover os atributos à cada usuário
- Muitos papers discutem como superar a necessidade de um servidor central
  - Existe uma solução, mas usuários são estáticos

Conclusão

- Problema ainda está em aberto

Conclusão

- Problema ainda está em aberto
- A criptografia baseada em atributos é promissora

Conclusão

- Problema ainda está em aberto
- A criptografia baseada em atributos é promissora
- O MPOTR é uma solução parcial relativamente consolidada

Trabalhos futuros

- Estudos da eficiência dos algoritmos

Trabalhos futuros

- Estudos da eficiência dos algoritmos
- Hipóteses matemáticas e aplicabilidade

Trabalhos futuros

- Estudos da eficiência dos algoritmos
- Hipóteses matemáticas e aplicabilidade
- Levantamento de soluções matemáticas para de criptografia para redes sociais

OBRIGADO

Um estudo sobre
conceitos criptográficos
aplicáveis em compartilhamento de informações em
rede social
com provedor de serviço não confiável

Adriano dos Reis Lopes
Orientador Prof. Dr. Paulo S. L. M. Barreto
Trabalho de formatura supervisionado
DCC IME USP