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

Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo
Brasil

Dezembro de 2014

Conteúdo

1 Introdução **1**

1.1 Objetivos 1

1.2 Motivação 1

1.3 Justificativa 2

1.4 Orientação do Estudo 2

2 O Estudo das redes sociais **3**

2.1 Estudo dos casos de uso 3

2.1.1 Informações de contatos 3

2.1.2 Conversas 4

2.1.3 Publicações pessoais 4

2.1.4 Publicações em página 5

3 O Estudo das soluções criptográficas **7**

3.1 O que é criptografia e pré-requisitos conceituais 7

3.2 Secure broadcasting using the secure lock 10

3.2.1 O que é criptografia de *broadcast* 10

3.2.2 O que é o *Secure lock* 11

3.2.3 Considerações gerais sobre o *Secure Lock* 11

3.3 Multi-party Off-the-Record Messaging (MPOTR) 12

3.3.1 O que é o OTR Messaging 12

3.3.2 O que é o MPOTR 12

3.3.3 Projeto de implementação do MPOTR 13

3.4 Attribute-Based Encryption 13

3.4.1 O que é ABE? Uma breve explicação 14
3.4.2 Uma visão geral sobre o desenvolvimento e os ramos do ABE . 15

4 Conclusão **20**
4.1 Sobre os estudos 20
4.2 Proposta de solução 20
4.3 Considerações finais 21

5 Trabalhos futuros **23**

6 Apreciação Subjetiva **25**
6.1 A motivação do trabalho 25
6.2 O desafio 25
6.3 O estudo 26
6.4 Sobre a disciplina do trabalho de conclusão 27
6.5 As conclusões pessoais 27

Bibliografia **29**

Lista de Figuras

3.1 Funcionamento conceitual do Método Diffie-Hellman de troca de chaves 10
3.2 Funcionamento conceitual do *Secure lock* 11

Lista de Tabelas

2.1 Permissões por ação e usuário de página 5

Capítulo 1

Introdução

1.1 Objetivos

Este trabalho de formatura supervisionado tem como objetivo utilizar os conhecimentos adquiridos no curso de Bacharelado em Ciência da Computação do IME USP para analisar soluções criptográficas para comunicação segura dentro de uma rede social onde, além de se poder estabelecer dinamicamente a confiança para um subgrupo de seu círculo de contatos, também o provedor de serviço não seja confiável, ou seja, onde o servidor não tenha conhecimento do conteúdo que é compartilhado pelos seus usuários.

1.2 Motivação

Hoje usa-se em larga escala redes sociais. Há dados que mostram que quase um terço dos brasileiros possui perfil no *Facebook* [1]. Com esse crescimento da comunicação via rede a privacidade das informações torna-se uma grande preocupação.
Se é demasiado afirmar a possibilidade de garantir a segurança dos dados em redes sociais, é ao menos possível apontar um norte de solução. O trabalho de conclusão de curso é um momento propício para tal estudo e por isso tal tema foi escolhido.
Os conhecimentos adquiridos no curso de ciência da computação no IME USP levaram a motivação para realização da análise de tal problema.

1.3 Justificativa

A utilização das redes sociais envolve diversos casos de uso onde informações pessoais sensíveis trafegam através da nuvem [2]. Os casos de espionagem realizados pelo governo estadunidense e divulgados por Snowden [3] mostraram ao mundo a relevância e a importância da proteção dos dados pessoais nos dias de hoje.

Dentre as redes sociais seguras de maior importância podemos citar a *Diáspora** [4]. O tráfego de informação nela é criptografado entre os servidores, mas o armazenamento em cada servidor não é necessariamente criptografado [5]. Por ser uma rede descentralizada é possível adicionar seu próprio servidor à rede e assim fazer o armazenamento das suas informaçõesm em servidor próprio. Ainda assim, a rede tem a fraqueza de depender da confiança no servidor. E é uma fraqueza, pois mesmo que se adicione à rede um servidor seguro próprio, na troca de informações suas mensagens podem passar por um servidor com más intenções. A situação se mostra crítica quando vemos notícias sobre a invasão de grandes servidores de provedores de serviços importantes [6] e mesmo de bancos [7], o que expõe o tamanho da fragilidade da *Diáspora**.

A junção de um elevado número de usuários de redes sociais com os casos de espionagem e a inexistência de uma solução realmente segura para compartilhamento de informações em redes sociais justificam o estudo de como proteger os dados das pessoas sem com isso modificar sua utilização cotidiana e sem precisar confiar no servidor, o qual pode ser também vítima de espionagem.

1.4 Orientação do Estudo

O estudo foi direcionado a fazer uma análise do uso das redes sociais e quais soluções criptográficas poderiam auxiliar na resolução do problema principal, que é garantir a privacidade dos dados em um ambiente com um servidor não confiável.

A partir da análise do funcionamento destas soluções criptográficas se buscará elencar o modo de uso e a possibilidade de uso para a solução do problema. Não será objetivo do presente trabalho a análise dos ataques que os sistemas podem sofrer, limitando-se a avaliação do que aparecerá nos próprios periódicos estudados.

Capítulo 2

O Estudo das redes sociais

Devido à popularidade que hoje tem o *Facebook* a análise de casos de uso foi baseada essencialmente nesta rede.

2.1 Estudo dos casos de uso

Analisando as funcionalidades disponíveis no *Facebook* e o uso cotidiano que se tem dessa ferramenta foi construído um cenário onde as ações permitidas são elencadas a seguir.

2.1.1 Informações de contatos

Tanto as pessoas quanto as páginas precisam ter informações que permitam sua identificação inicial. Aqui não se trata de algum tipo de chave pública, mas sim de informações como nome da pessoa, idade, em que colégio estudou etc. Tal tipo de informação deverá servir de apresentação que permita às pessoas se encontrarem dentro da rede social. Como tarefa mínima de segurança, deverá ser permitido que apenas quem pertença a rede social possa buscar tais informações.

2.1.2 Conversas

Conversa direta (peer-to-peer)

Conversa comum, como uma conversa telefônica (comunicação imediata) ou uma troca de e-mails (comunicação mediata). Aqui se encaixam os *chats* simples.

Conversa em círculo de contatos

Conversa em grupo onde só poderá haver pessoas de confiança de todos. Em outras palavras, todas as pessoas na conversa precisam ser contatos de todas as outras. Isso irá garantir um nível de segurança maior para a conversa.

Conversa em grupo geral

Aqui haverá uma conversa mais geral com outras pessoas para além dos contatos de uma pessoa. Mesmo não sendo um circulo fechado, o grupo é fechado em si, ou seja, quem não está no grupo não pode visualizar as informações da conversa.

2.1.3 Publicações pessoais

É comum nas redes sociais que cada pessoa faça publicações para compartilhar com seus contatos. Em geral, determinados conteúdos serão compartilhados para todos os amigos e outros apenas para uma parcela. Quem poderá visualizar cada uma de suas publicações é o ponto determinante da privacidade que a pessoa poderá ter ou não.
Dentre as ações, serão permitidas:

Publicação pessoal para parcela de contatos

A pessoa deverá poder escolher quem irá visualizar a publicação, tendo como opção toda sua lista de contatos ou apenas uma parcela determinada.

Fazer comentário em publicação de contato

Caso a pessoa deseje comentar alguma publicação de uma página, as regras serão seguidas como definidas pela própria página. No caso da publicação ser de um

contato, a possibilidade de visualização do comentário deve ser igual ao da leitura para aquela publicação, ou seja, só os que podem ler a publicação poderão comentar e ler os demais comentários.

2.1.4 Publicações em página

Uma página é definida por representar determinado tema, empresa, grupo etc., e por publicar conteúdo para uma grande parcela de pessoas (em geral, o máximo que puder atingir). Nela há três tipos de interações possíveis: administrar, moderar e seguir. Todas as pessoas poderão visualizar as publicações da página e poderão ter um papel associado a ela. A tabela abaixo mostra os papéis e suas funções:

Tabela 2.1: Permissões por ação e usuário de página

Atividade	**Administrador**	**Moderador**	**Seguidor**
Excluir página	✓	✗	✗
Adicionar novos moderadores	✓	✗	✗
Adicionar novos seguidores	✓	✓	✗
Publicar conteúdo na página	✓	✓	✗
Avaliar/comentar conteúdo	✓	✓	✓
Ler comentários/avaliações	✓	✓	✓

Das atividades gerais da página, temos as seguintes:

Publicação em nome da página

Os moderadores de páginas podem disponibilizar conteúdo para todos os seguidores em nome da página, ou seja, o conteúdo publicado é assinado pela página e não pelo moderador.

Publicação pessoal na página através de comentários

Para permitir uma discussão sobre os conteúdos publicados pela página, deve haver espaço para comentários. Tais comentários só deverão ser escritos por administrado-

res, moderadores ou seguidores (aqueles que recebem as publicações regularmente), pois este mecanismo é usado para aumentar o número de seguidores da página.

Capítulo 3

O Estudo das soluções criptográficas

3.1 O que é criptografia e pré-requisitos conceituais

No cenário estabelecido por este TCC, todas as informações pessoais precisam ser assinadas e criptografadas levando em consideração que o servidor provedor da rede social não é confiável. Possíveis comunicações abertas/públicas não são abordadas por fugir do escopo do trabalho.

A preocupação aqui é verificar os sistemas criptográficos que podem fornecer um aparato para permitir que somente os que tenham autorização consigam extrair as informações dos dados e que os que não tenham permissão não possam extrair as informações mesmo com os dados [criptografados] em mãos. Isso se contrapõe a um servidor confiável que irá fazer a verificação de acesso e então prover os dados, pois no escopo do trabalho o simples acesso aos dados não garante a extração das informações neles contido.

O recorte feito para os sistemas criptográficos a serem estudados baseou-se nos seguintes artigos: Secure broadcasting using the secure lock [8]; Multi-party Off-the-Record Messaging [9]; e uma vasta literatura sobre criptografia baseada em atributos.

Abaixo estão listados os conceitos ligados à criptografia que serão utilizados na explicação dos esquemas de criptografia.

Criptografia / Encryption

Ação de esconder as informações de uma mensagem, fazendo com que apenas aqueles que possuam uma (ou mais) chave possam ter acesso ao conteúdo da mensagem.

Exemplo: Alice envia um e-mail criptografado a Bob. Se Charlie conseguir obter tal e-mail ele não conseguirá ler seu conteúdo, porque Charlie não é Bob e não possui a chave de decriptografia.

Autenticação / Authentication

Garantia de que uma mensagem foi enviada pelo remetente que a assina.

Exemplo: Alice envia uma mensagem assinada para Bob. Devido a autenticação (assinatura) Bob tem certeza de que foi Alice, e não Charlie, que lhe mandou a mensagem

Segredo contínuo / Perfect Forward Secrecy

Rapidamente após Bob receber uma mensagem ela se torna ilegível para todos em qualquer lugar. [10]

Exemplo: Alice e Bob conversam diariamente através de um correio de mensagens instantânea. A cada novo dia ninguém tem acesso às conversas passadas; nem mesmo Bob ou Alice, caso estes não tenham guardado a conversa decriptografada.

Negabilidade / Deniability

Capacidade de negar a autoria das mensagens, inexistência de uma prova de autoria.

Exemplo: Após uma conversa, embora Bob esteja certo de que a mensagem veio da Alice, ele não pode convencer Charlie de tal fato. Além disso, Charlie poderia forjar transcrições de conversas falsas (entre Bob e Alice) tão precisas quanto uma real. [10]

Resistência a conspiração / collusion resistance

A criptografia não pode ser quebrada mesmo que um subconjunto de usuários, dos quais não participa um que tem a chave de decriptografia, tente quebrá-la. **Exemplo:** Uma mensagem para ser decriptografada por um usuário necessita que ele tenha os atributos "professor"e "USP". Se Alice possui o atributo "professor"e Bob o atributo "USP", mas nenhum possui ambos, então mesmo que Alice e Bob se juntem, eles não poderão decriptografar tal mensagem.

Revogação de atributo/ Atributte revocation

Possibilidade de um usuário no sistema perder um de seus atributos.

Exemplo: Alice tem o atributo "estudante da USP". Quando ela se formar, perderá esse atributo. Neste exemplo, a revogação de atributos é então a capacidade do sistema em retirar de Alice o atributo "estudante da USP"

Modelo de oráculo aleatório / random oracle model [11]

Modelo de prova matemática de segurança criptográfica baseado no oráculo aleatório. O oráculo funciona da seguinte forma: solicitações lhe são feitas com um valor de entrada e ele responde com um valor de saída. Quando uma solicitação é feita ele verifica se o dado que lhe foi fornecido como entrada já havia sido solicitado em outro momento anterior. Se sim, ele devolve o mesmo valor de saída que foi utilizado para aquele valor de entrada. Se não, ele sorteia com distribuição uniforme um novo valor e o devolve como valor de saída.

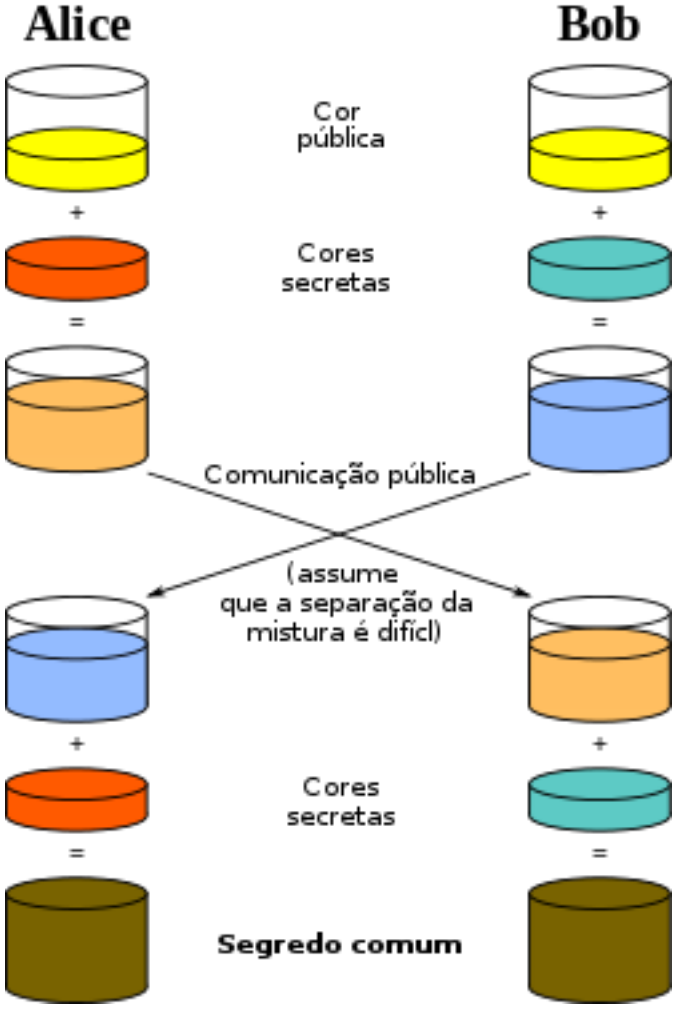
Segurança adaptativa/Adaptively Secure

Segurança adaptativa é uma noção utilizada para dizer que um esquema de criptografia garante segurança, ou seja, não revela nenhuma informação, mesmo em um esquema interativo onde participantes podem adaptativamente ser corrompidos durante o processo de execução. [12]

Método Diffie-Hellman de troca de chaves/Diffie-Hellman Key-Exchange

Este método de troca de chaves é utilizado para criar um canal de troca de informações seguro através de um canal inseguro. A partir de uma chave pública comum dois usuários criam uma composição de uma nova chave que será de conhecimento só de ambos. A imagem a seguir, adaptada de [13], exemplifica como isso é feito.

Figura 3.1: Funcionamento conceitual do Método Diffie-Hellman de troca de chaves



3.2 Secure broadcasting using the secure lock

3.2.1 O que é criptografia de *broadcast*

Considere um cenário onde há um provedor centralizado de informações e um conjunto de usuários que recebem o conteúdo provido por ele. A criptografia de *broadcast* é a que permite que esse servidor, através da distribuição de chaves criptográficas pré-definidas, possa enviar uma mensagem a qualquer subgrupo de

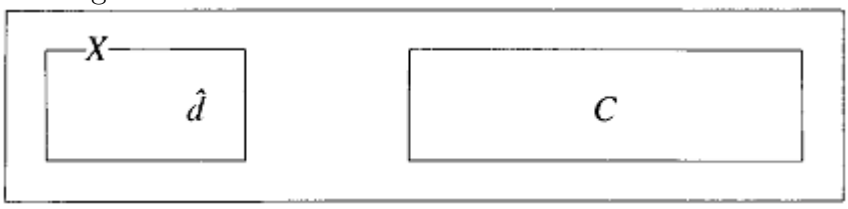
usuários sem que os demais, ou alguém externo aos usuários, possam ter qualquer conhecimento sobre a mensagem enviada [14].

3.2.2 O que é o *Secure lock*

Como na criptografia de *broadcast* as mensagens são enviadas de um servidor central para todos os usuários, é preciso uma modificação no protocolo para que seja possível que este servidor envie mensagens a subgrupos quaisquer, que podem mudar dinamicamente.

A proposta do *secure lock* é que exista uma chave de sessão protegida pelo *lock*, a qual permita que apenas um subgrupo selecionado dos usuários possa acessar a chave de sessão e então decriptografar a mensagem original [8]. A imagem abaixo mostra como funciona conceitualmente o *secure lock*.

Figura 3.2: Funcionamento conceitual do *Secure lock*



Onde:

X é o *lock*

$\hat{\mathbf{d}}$ é a chave da sessão de decriptografia

C é a mensagem original criptografada

3.2.3 Considerações gerais sobre o *Secure Lock*

Este protocolo utiliza o Teorema Chinês do Resto [15] para conseguir criar o *lock*. Para isso, é preciso que um servidor centralizado distribuia as chaves criptográficas a cada usuário, que neste caso seriam números primos grandes. A encriptação depende do conhecimento de cada chave, enquanto que a decriptação depende apenas do conhecimento de sua própria chave.

A dependência do conhecimento de cada chave para a distribuição da mensagem para um determinado subgrupo de usuário faz com que seja preciso um servidor centralizado que tenha esse conhecimento. Isso quebra a premissa assumida no presente estudo de se ter um servidor não confiável. Para contornar isso, cada usuário poderia ter uma chave específica para cada contato que tivesse. Porém isso demandaria um número de chaves demasiado grande para serem gerenciadas, o que torna tal solução ineficiente.

3.3 Multi-party Off-the-Record Messaging (MPOTR)

3.3.1 O que é o OTR Messaging

O "Off-the-Record Messaging"(OTR), que poderíamos traduzir como "conversa fora de registro", é um protocolo desenvolvido por Borisov, Goldberg e Brewer construído para permitir conversas privadas através de um mensageiro instantâneo provendo: privacidade, autenticidade, segredo contínuo e negabilidade de autoria. [10]

O protocolo OTR consiste em duas fases: a primeira onde uma troca de chaves de autenticação é realizada obtendo uma chave de sessão compartilhada, usando o método de Diffie-Hellman de troca de chaves; a segunda consistindo de uma contínua atualização da chave de sessão durante a troca de mensagens do mensageiro instantâneo [16].

3.3.2 O que é o MPOTR

Com a limitação do "OTR messaging"de servir apenas à conversas ponto a ponto, ou seja, entre duas pessoas, ficava em aberto o problema de expandí-lo para uma conversa com múltiplas pessoas. O MPOTR (Conversa fora de registro com múltiplos participantes, em tradução livre) foi então desenvolvido para responder a essa limitação.

Uma tentativa de estender o OTR para conversas com mais de dois participantes foi feita por Bian, Seker e Topaloglu. O crucial da solução deles é que um dos usuários fica designado como um "servidor virtual". Enquanto isso é plausível de se

fazer facilmente sobre determinadas circunstâncias, ela desvia do objetivo original do OTR, que é imitar uma conversa privada real. Em um conversa privada em grupo não há um servidor virtual responsável por facilitar a conversa. Ademais, o servidor se torna uma entidade alvo para participantes mal intencionados. Finalmente, assume-se que o servidor tem que ser honesto, pois um servidor desonesto pode comprometer ambas confidencialidade e integridade de todos as mensagens enviadas durante a sessão do *chat* [9].

O protocolo MPOTR foi proposto por Goldberg, Gundy, Ustaoglu e Chen em [9]. Nele se mantém os requisitos do *OTR messaging*, porém aplicados agora para grupos de conversas de tamanho arbitrário sem, contudo, necessitar de um "servidor virtual". Parte do design foi refeito, pois, por exemplo, a negabilidade de autoria tem um sentido diferente em uma conversa em grupo. Neste caso não se nega a participação na conversa, nega-se o conteúdo das mensagens e deixa-se em aberto em qual das conversas em grupo o usuário estava participando.

3.3.3 Projeto de implementação do MPOTR

Existe um projeto de implementação do MPOTR aberto, cuja apresentação encontra-se disponível em [17].

Deste protocolo é importante notar que, apesar de todo o esforço feito para conseguir atender às necessidades de uma comunição segura, o projeto de sistema criptográfico ainda carece de prova de segurança, de um estudo acadêmico/científico rigoroso. Por isso, os conceitos aqui elencados nos ajudam a entender as necessidades do nosso sistema e que já existe algumas tentativas de respondê-los. Como o TCC é de estudo e não se pretende implementar o sistema, a análise do MPTOR é útil. [17]

3.4 Attribute-Based Encryption

Os primórdios do ABE: o *Identity based encryption*

Pensada por Adi Shamir em [18], a criptografia baseada em identidade (IBE, na sigla em inglês) tinha a ideia simples de que cada pessoa poderia ter uma identi-

dade (chamada naquele momento de "smart card") e a partir dela poderia enviar informação de maneira privada para outra que possuísse também uma identidade naquela rede.

O IBE funciona através de uma entidade central, uma entidade certificadora, que distribui as identidades, os "smart cards". Quando um usuário entra na rede ele recebe sua identidade, não sendo nunca mais preciso recriá-la ou adaptá-la. No processo de criptografia e decriptografia também não é necessária a ação da entidade central. Depois de gerar as identidades o papel da entidade central desaparece, não sendo ela mais necessária.

O IBE unifica os processos de criptografia e de assinatura, ou seja, de uma só vez esconde os dados de forma que somente o destinatário possa verificar seu conteúdo e ainda garante a assinatura do remetente.

Como um dos frutos do desenvolvimento da criptografia baseada em identidade surge pela primeira vez, em [19], o conceito de criptografia baseada em atributos (ABE na siglas em inglês). O *Fuzzy*-IBE busca desenvolver a criptografia baseada em identidade para o reconhecimento biométrico. Neste contexto é preciso que sejam reconhecidas características/atributos das pessoas, mas que sejam toleráveis pequenas falhas, pequenas pertubações, ou seja, tolerante a erros. Como a base desta criptografia passa a ser atributos das pessoas, advém quase que naturalmente o desenvolvimento de uma criptografia baseada em atributos, a qual chamamos de ABE.

Novos requisitos passam a ser determinantes para o funcionamento seguro de sistemas baseados em atributos: não pode ser possível a decriptografia de determinada informação com a soma de atributos de pessoas diferentes, ou seja, é necessário que uma única pessoa satisfaça todos os atributos da informação criptografada para que se possa decriptografá-la. Essa preocupação, chamada em geral de resistência contra conspiração, torna-se um dos aspectos centrais de tal criptografia.

3.4.1 O que é ABE? Uma breve explicação

Em poucas palavras podemos dizer que "attribute-based encryption"(ABE, criptografia baseada em atributos) é um tipo de criptografia que permite que os usuários

possam acessar somente as informações cujos seus atributos satisfaçam a política de segurança delas.

Imagine a seguinte situação: o professor Routo Terada quer disponibilizar as notas finais aos seus alunos da disciplina de criptografia do IME-USP do primeiro semestre de 2014 e gostaria que somente os alunos matriculados nesta disciplina (MAC0336) pudessem vê-las. Então precisaríamos que somente aqueles que possuam os atributos "aluno", "matriculado MAC0336-01/14", "IME"e "USP"ou possua os atributos "professor MAC0336-01/14", "IME"e "USP"tenham acesso às notas.

A criptografia baseada em atributos pode solucionar este problema, pois as chaves de cada usuário estão vinculadas a um conjunto de atributos. Ao se criptografar uma mensagem (como as notas dos alunos) utiliza-se uma política de acesso que irá descrever os atributos necessários que permitam a decriptografia da mensagem. No nosso caso poderíamos utilizar a política: (("aluno"E "matriculado MAC0336-01/14") OU ("professor MAC0336-01/14")) E "IME"E "USP".

Surge com esse tipo de criptografia a preocupação de proteção contra a conspiração de usuários. Em outras palavras, o ABE deve garantir que não se possa mesclar atributos de usuários diferentes para conseguir decriptografar uma mensagem. Voltando ao nosso exemplo, imagine que Alice possui os atributos "aluno", "IME"e "USP", e que Beto possua os atributos "aluno", "matriculado MAC0336-01/14"e "UNICAMP". Se Alice e Beto se juntarem para verificar as notas dos alunos de criptografia do IME USP irão conseguir? O sistema criptográfico é construído de maneira a não permitir isso. Em outras palavras, a mensagem só pode ser decriptografada por um usuário, uma identidade, que satisfaça toda a política de acesso da mensagem, não sendo possível unificar atributos de usuários diferentes para realizar tal tarefa.

3.4.2 Uma visão geral sobre o desenvolvimento e os ramos do ABE

Os estudos realizados revelaram uma extensa literatura sobre a criptografia baseada em atributos. Em seguida busca-se trazer uma visão geral àqueles que tiveram seu

primeiro contato com este tipo de criptografia no presente trabalho. As dificuldades técnicas de implementação não serão, em geral, abordadas aqui. Será feita uma breve passagem pelas referências [20] [21] [22] [23] [24] [25] [26] [27], de maneira a construir o desenvolvimento dos esquemas de criptografia baseada em atributos.

Multi-authority attribute-based encryption

O esquema de criptografia baseada em atributo apresentado em [19] foi construído com base em uma única autoridade provedora de atributos. Como seguia o esquema da criptografia baseada em identidade, cada usuário recebia sua chave de decriptografia de uma entidade certificadora, a qual deveria ser confiável desde que ela possui sua chave de decriptografia, pois foi esta entidade quem gerou a chave [20]. Ficou então em aberto o problema de se ter múltiplas autoridades provedoras de atributos, a qual o esquema desenvolvido por Chase [20] vem responder com entidades múltiplas e independentes.

Vamos imaginar a seguinte situação: uma entidade de fomento quer disponibilizar o resultado de uma avaliação apenas para professores que lecionem em ao menos duas universidades. Sendo cada universidade uma entidade provedora de atributos, então temos a situação de que para decriptografar o resultado da avaliação o usuário precisa satisfazer o atributo de "professor"em ao menos duas das $\boldsymbol{n}$ universidades existentes. Aqui cada universidade é uma entidade independente. Então mesmo que uma entidade seja violada/corrompida, ainda assim se garantirá o sigilo das informações.

De maneira geral a criptografia baseada em atributos com múltiplas autoridades permite que aquele que criptografa uma informação defina quantos atributos (e até quais) precisam ser satisfeitos para cada entidade e qual é o número mínimo de entidades na qual precisa satisfazer os atributos para que a informação seja decriptografada.

Até aqui ainda é preciso de uma identificação geral no sistema (chamado no *paper* de ***GID*** - global identification), a qual deve ser única, não podendo ser reivindicada por outro usuário. Além disso, cada autoridade provedora de atributos deve poder

verificar a identidade do usuário. Este segundo requisito é necessário para que as entidades provedoras de atributos possam evitar a concessão de autorização para grupos de usuários quando não existe comunicação entre as entidades, ou seja, para evitar o ataque por conspiração.

A concessão de atributos neste cenário está vinculada a GID do usuário. Isso implica na necessidade de uma entidade central que forneça as GIDs. Apesar desta entidade não estar vinculada à concessão de atributos aos usuários, como parte central do sistema, ela tem a capacidade de decriptografar todas as informações. Em outras palavras, um dos requisitos deste esquema é ter uma entidade central confiável.

A limitação da autoridade central é tratada, mas não totalmente resolvida, no *paper* [23]. A técnica neste caso é remover a autoridade central fazendo com que um usuário precise ter os atributos para a mensagem criptografada satisfeitos em $t+1$ autoridades provedoras de atributos, onde $t < n/2$ e $\boldsymbol{n}$ é o número total de autoridades.

Ciphertext-policy attribute-based encryption

Na criptografia baseada em atributos com política de texto cifrada (Ciphertext-policy attribute-based encryption, CP-ABE) busca-se colocar a verificação do atendimento da política de criptografia embutida diretamente no dado criptografado e não mais em um servidor. Ou seja, quando se vai criptografar um dado define-se qual é a política de acesso (baseada em atributos) que permitirá a decriptografia. Isso vem justamente para tentar eliminar a necessidade de confiança nos servidores de validação.

Quando utilizamos o servidor para armazenar as informações localmente e usamos as chaves criptográficas apenas para verificar se o usuário tem atributos suficientes para acessá-la, como colocada tradicionalmente no esquema da ABE, acabamos por ficar refém da confiança neste servidor. A motivação colocada em [21] é justamente a de que cada vez mais as informações são armazenada em servidores distribuídos, devido ao volumoso aumento na quantidade de dados armazenados. Embora a distribuição da informação em diversos servidores venha a garantir um melhor desempenho do sistema, isso aumenta drasticamente o risco de comprometimento dos dados, pois

agora não é apenas um servidor que precisa ser confiável, mas sim todos os servidores que estão distribuindo a informação.

Vale ressaltar também que um outro esquema chamado *Key-policy ABE* (KP-ABE), que surgiu anteriormente a este, tem um funcionamento inverso: nos dados criptografados se embute os atributos e na identificação se coloca a política de acesso.

Por fim, para aqueles que queiram aprofundar no estudo da implementação deste tipo de sistema a referência [22] coloca a CP-ABE de uma maneira mais geral quanto à implementação e algoritmos criptográficos.

Decentralizing attribute-based encryption

Em [24] uma nova contribuição é feita: um sistema de criptografia baseada em atributos sem uma autoridade central permanente e onde cada parte pode se tornar um servidor de atributos. Neste sistema só é necessário uma autoridade central durante a fase de criação dos parâmetros de referência do sistema. Esta fase inicial precisa ser confiável.

Um participante pode simplesmente agir como uma autoridade servidora de atributos criando uma chave pública e distribuindo atributos relacionados à si. Autoridades de atributos diferentes não precisam ter conhecimento das outras. Os parâmetros globais do sistema são usados para criar uma identificação única para cada autoridade.

Com os parâmetros públicos qualquer um pode criptografar dados com uma fórmula *booleana* baseada nos atributos das autoridades.

Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption without Random Oracles

Estudo feito por [25] busca ser um desenvolvimento do [24]. Diz: "*Embora seu sistema se torne ineficiente para um universo de grande quantidade de atributos, ele é o primeiro sistema de criptografia baseada em atributos com múltiplas autoridades que é totalmente seguro e tem prova de segurança no modelo do oráculo aleatório*" [25] (tradução livre). Apesar deste novo sistema de criptografia se colocar no modelo de complexidade padrão, e não mais no modelo do oráculo aleatório, e com uma

melhora em relação a eficiência com grande número de atributos, ele necessita de múltiplas autoridades centrais, que são separadas das autoridades provedores de atributos neste caso. Isso acaba por nos levar de volta à necessidade de confiança em servidores, que agora, ao invés de somente um, precisa de diversos servidores corrompidos conspirando para quebrar os dados criptografados.

Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption

Um dos pontos sensíveis na ABE é que durante a validação dos atributos há uma exposição da identificação do usuário. Isso pode ser usado, por exemplo, por uma autoridade provedora de atributos corrompida para pegar informações sobre quais são os atributos de um usuário com o qual interagiu. Chase e Chow em [26] elaboram um sistema onde o GID do usuário não é revelado no processo de validação dos atributos com a entidade, além de avançar do sistema anterior de Chase [20] para um verdadeiro sistema descentralizado.

Este *paper* traz uma nova contribuição que é a construção de um sistema que responda a um problema que foi deixado em aberto por Chase e Chow, de que seu sistema não necessitasse da cooperação entre as autoridades continuando a preservar a identidade [27]. Este é um KP-ABE baseada na hipótese padrão de complexidade.

Capítulo 4

Conclusão

4.1 Sobre os estudos

O *Secure lock* foi um ponto de partida do estudo por ter sido utilizado no trabalho de Hilder Vitor Lima Pereira, em seu TCC do IME USP em 2013 [28]. Serviu para o entendimento dos conceitos ligados à criptografia de *broadcast*, o qual permitiu o aprofundamento dos estudos.

O estudo do MPOTR foi muito rico, pois diferente de estudos acadêmicos, seus desenvolvedores buscam os problemas reais levantados no uso cotidiano e sempre levantam os problemas de implementação das tecnologias. Isto é interessante, pois nem sempre o que se consegue no plano teórico se consegue no plano prático. Porém faltam provas matemáticas rigorosas de que seu sistema realmente funciona sem falhas.

Por fim, o estudo da criptografia baseada em atributos foi o que se mostrou mais desenvolvido teoricamente e mais próximo do compartilhamento de informações em redes sociais. Sem dúvida foi o mais enriquecedor para o entendimento dos desafios atuais da criptografia.

4.2 Proposta de solução

O vasto estudo realizado, principalmente quanto à criptografia baseada em atributos mostrou que ainda não há uma solução factível para o problema levantado por este

trabalho de formatura. Apesar de não haver condições de propor um sistema que o resolva diversas características e funcionalidades dos protocolos e sistemas estudados ao menos apontam um caminho, como já era imaginado quando se fechou esta proposta de trabalho.

O *Secure lock* serviu de ponto de partida dos estudos, porém não serve ao objetivo do trabalho. Isso porque ele depende necessariamente de um servidor que distribua as chaves criptográficas. Em outras palavras, seu mecanismo depende da confiança no servidor, o que quebra uma das premissas do sistema almejado.

O MPOTR serve parcialmente ao sistema. Isso porque este protocolo objetiva servir à conversas instantâneas. Nesse ponto, ele resolve toda a parte do estudo de casos de uso de "conversas". Além disso poderia ser facilmente aplicado ao sistema, pois ele foi pensado e desenvolvido desde o seu início já com sua implementação prática. A grande questão é que os demais pontos ficam ainda em aberto.

A criptografia baseada em atributos apesar de ainda não servir à proposta de sistema e ainda estar no campo de desenvolvimento teórico, não de implementação, é o conceito mais promissor do que possa vir a ser usado em um sistema de rede social com provedor de serviço não confiável.

4.3 Considerações finais

A criptografia baseada em atributos poderia resolver todos os pontos ainda em aberto para o sistema caso contasse com um provedor de serviço confiável ou se na criação já se tivesse todos os participantes interagindo. Uma de suas limitações é que, para manter um sistema seguro, todos os usuários devem estar definidos na criação do sistema. Segundo os conhecimentos adquiridos nos estudos deste trabalho, ainda é um problema em aberto ter um sistema criptográfico baseado em atributos sem uma autoridade central permanente que consiga adicionar usuários ao longo do tempo. Criar usuários fictícios inicialmente e distribuí-los à medida que novas pessoas entram no sistema, tornando estes usuários reais, quebra o princípio básico de segurança, pois o distribuidor das identidades pode se passar por qualquer

uma destas identidades.

Muitas limitações da criptografia baseada em atributos foram e vêm sendo solucionadas, mas ainda não se atingiu a independência em relação a um (ou mais) servidor central. Outro ponto que merece atenção, e que também dificulta a remoção do servidor central, é a necessidade do sistema prover a revogação de atributos, o que é muito comum no caso das redes sociais e faz parte do nosso caso de uso (desde a exclusão de amigos até a remoção de moderadores e seguidores das páginas).

Ainda vale apontar um trabalho recente, de julho de 2014, de Huang, Ma, Yang, Fu e Niu [29] chamado "*Secure Data Sharing and Retrieval Using Attribute-Based Encryption in Cloud-Based OSNs*", que podemos traduzir para algo como "*Compartilhamento e recuperação segura de dados usando ABE em rede sociais 'on-line' baseadas em nuvem*". Não foi possível aprofundar seu estudo devido ao tempo disponível restante do trabalho, porém ele busca uma resposta a um problema semelhante ao colocado por este trabalho. A diferença é justamente não ter como objetivo uma rede social com um provedor de serviço não confiável.

Capítulo 5

Trabalhos futuros

Com a riqueza dos estudos aqui tratado, alguns pontos não foram devidamente aprofundados e podem ser de grande valia para a proposição inicial do trabalho. A leitura da introdução de [27] será de grande valia, pois faz um resumo das principais características dos sistemas de ABE desenvolvidos até então e garante um panorama geral àqueles que desejam aprofundar os estudos.
Abaixo ficam elencados pontos que podem ser desenvolvidos como continuidade deste trabalho:

Eficiência dos algoritmos e aplicabilidade

Principalmente pelo estudo feito sobre o MPOTR ficou visível a distância entre os sistemas criptográficos teóricos/acadêmicos e sua aplicabilidade. Implementar os sistemas de criptografia, definir protocolos e torná-los utilizáveis é uma tarefa talvez tão grande quanto desenvolver os sistemas matemáticos. A medida do que é razoável como eficiente ou não também é algo que não é mensurável sem um duro trabalho de verificação de aplicabilidade e de recursos disponíveis a nível de usuários ao redor do mundo, muito embora a eficiência do sistema possa ser trabalhada desde o esboço do sistema criptográfico.

Hipóteses utilizadas e seu impacto na segurança da aplicação

Novamente o trabalho dos desenvolvedores do *OTR messaging* e MPOTR mostra que um sistema ideal pode não ser de serventia alguma quando falamos de

usuários reais. Diversas premissas que têm importância no cotidiano, como o sigilo contínuo (*Perfect Foward Secrecy*), acabam não sendo o foco do desenvolvimento matemático acadêmico dos sistemas. Um exemplo disso é ver que o modelo do oráculo aleatório é matematicamente plausível, mas na prática não traz a segurança necessária, pois tal oráculo não existe [ainda].

A noção de segurança adaptativa, que aparece pela primeira vez em [30], é outro ponto onde a segurança pode ser quebrada na aplicação real, ou seja, é necessário considerar todas as variáveis e formas possíveis quanto às tentativas de espionagem.

Estudo do que já foi desenvolvido sobre as redes sociais

O estudo mais aprofundado de [29] pode, e certamente o fará, levar a um melhoramento no estudo do que já está em desenvolvimento, a nível acadêmico, quanto aos sistemas criptográficos para rede sociais. Uma pesquisa pela palavra chave *OSN* (*Online social network*) irá trazer uma boa bibliografia relacionada ao tema de rede sociais seguras. Aqui está também um leque para novas definições de requisitos do sistema.

Capítulo 6

Apreciação Subjetiva

6.1 A motivação do trabalho

A falta de privacidade na internet sempre me deixou incomodado. O relato de alguns amigos de falsos sequestros que eram feitos com dados obtidos através das redes sociais agravava isso. Quando tive contato com criptografia, vi que existia, de alguma maneira, uma solução para tal problema. Foi então que me motivei a fazer um estudo sobre criptografia para redes sociais. Um "detalhe" importante do trabalho foi a busca por garantir privacidade de fato. Então foi que incluí no estudo o ponto de "não confiança no provedor de serviço". Os casos de espionagem dos Estados, dentro os quais os EUA são o maior exemplo, vem justamente na contramão disso. Um bom exemplo foi a luta "anti-terrorista" depois dos ataques às torres gêmeas que foi usada como justificativa para quebrar a privacidade de qualquer um.

Em suma, minha motivação foi a de que as pessoas pudessem usar as redes sociais com a liberdade que têm na vida real, sem ter que se preocupar em serem espionadas por estarem no meio virtual.

6.2 O desafio

Quando pensei em começar o trabalho tive a ilusão de que seria possível, se não implementar todo o software para tal tipo de rede, pelo menos apontar o caminho.

Quando comecei os estudos vi que o "detalhe" da não confiança no provedor de serviço era um problema em aberto e que a dificuldade de alcançar isso era grande. Era quase como o último teorema de Fermat, com um enunciado simples e de fácil entendimento, mas de resposta muito complexa.

6.3 O estudo

Iniciei os estudos com o que eu conhecia do trabalho feito por um amigo. Ele havia implementado um sistema de criptografia para o *Facebook* através de um complemento para o *Google Chrome*. Então comecei a estudar a criptografia de *broadcast*. O conceito é simples, porém exige um conhecimento básico do que é criptografia. Já neste início percebi que a disciplina optativa eletiva que fiz no IME de criptografia foi fundamental.

Ainda no primeiro semestre de 2014 ocorreu em São Paulo um evento de criptografia que foi importante ao meu trabalho: a *Cryptorave*. Foi um ciclo de palestra e oficinas que tratava sobre como um usuário comum poderia ter privacidade na rede com o que existe de criptografia implementada hoje e qual é o estado da arte de criptografia. Foi meu primeiro contato com o protocolo OTR, que fez parte do meu estudo.

Passado tal evento, fui pesquisar sobre redes sociais seguras. Foi quando percebi o que já desconfiava: não existia nenhuma rede social com as características que eu buscava. A *Diáspora**, única rede social que encontrei com a preocupação com a privacidade dos usuários, se baseava na distribuição dos provedores de serviço para garantir a segurança. Ou seja, parte da segurança da rede era delegada aos usuários, que poderiam adicionar um servidor próprio. Como meu estudo já havia mostrado que é praticamente impossível garantir segurança permanente confiando que um determinado servidor não será invadido, a *Diáspora** fugia do que eu almejava.

Tive bastante dificuldade em encontrar exatamente o que precisava para redes sociais. Demorei para encontrar a criptografia baseada em atributos e entendê-la. Apesar disso, foi justamente ela o que mais estudei e o que mais me ajudou com o trabalho. Foi com ela que consegui entender melhor o que era simples e o que

era mais complexo quanto à criptografia. Por exemplo: a junção em um sistema de criptografia da propriedade de não ter um servidor central que tenha conhecimento das informações com a propriedade de poder adicionar e excluir membros torna o problema criptográfico a ser resolvido muito complexo.

6.4 Sobre a disciplina do trabalho de conclusão

Muitos estudantes já sabiam o que gostaria de fazer em seu trabalho antes mesmo de se matricular na disciplina e já tinham conversado com os professores que iriam orientá-los. Outros, como foi o meu caso, passaram a pensar nisso somente quando se matricularam na disciplina. Ao final do ano fizemos nossas apresentações com o que conseguimos fazer, com o fruto do trabalho do ano todo. Acredito que esse momento seria muito útil para aqueles que pretendem fazer a disciplina no próximo ano, pois poderiam ver os trabalhos e conversar com as pessoas sobre a experiência que tiveram (desde as dificuldades, até o estilo de trabalho de cada orientador), enriquecendo assim os futuros trabalhos de conclusão de curso.

Outro ponto que me pareceu importante foram as entregas parciais. Talvez se houvesse uma primeira apresentação do trabalho de cada um no meio do ano isso potenciaria os trabalhos e ajudaria aqueles que têm dificuldades com as apresentações.

6.5 As conclusões pessoais

A maior experiência que ganhei com o trabalho foi justamente fazer algo que não era um trabalho pré-fabricado por um professor, mas algo que foi uma ideia própria (mesmo que não original). Para aqueles que pretendem fazer um mestrado, essa é uma experiência importante, pois é a primeira experiência "autônoma" do estudante.

Ainda considero muito importante a pesquisa que iniciei. Porém, vejo que o desenvolvimento matemático necessário para conseguir resolver o problema proposto me foge às capacidades atuais. Há possibilidade de continuação da pesquisa, pois nem toda a literatura sobre o tema eu pude esgotar e a cada dia novos *papers* sobre o

tema têm surgido. Mesmo diante das dificuldades, vejo que as redes sociais seguras ainda são uma necessidade geral.

Bibliografia

[1] Socialbakers.com (2014), *http://www.socialbakers.com/blog/1290-10-fastest-growing-countries-on-facebook-in-2012*

[2] Infowester.com (2014), *Computação em nuvem - http://www.infowester.com/cloudcomputing.php Acesso em 01/09/2014*

[3] g1.globo.com (2014), *Entenda o caso de Edward Snowden, que revelou espionagem dos EUA - http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html Acesso em 20/08/2014*

[4] diasporafoundation.org (2014) *Rede descentralizada diáspora. - http://diasporafoundation.org. Acesso em 08/09/2014*

[5] Protocolo da federação diáspora (2014) *Wiki diáspora*. - https://wiki.diasporafoundation.org/Federation_protocol_overview Acesso em 08/09/2014*

[6] g1.globo.com (2014), *Inteligência dos EUA invadiu data centers de Google e Yahoo, diz jornal - http://g1.globo.com/mundo/noticia/2013/10/inteligencia-dos-eua-invadiu-data-centers-de-google-e-yahoo-diz-jornal.html Acesso em 20/08/2014*

[7] br.reuters.com (2014) *JP Morgan descobre violação de dados por hackers, diz mídia - http://br.reuters.com/article/internetNews/idBRKBN0IN0VQ20141103 Acesso em 03/11/2014*

[8] G.-H. C. W.-T. Chen, (1989) *Secure broadcasting using the secure lock - IEEE Transactions of Software Engineering, vol. 5, no. 8, pp. 929–934.*

[9] Goldberg I., Gundy M. D. V., Ustaoglu B. e Chen H. (2009) *Multi-party off-the-record messaging - Proceedings of the 16th ACM conference on Computer and communications security*, Chicago, Illinois, EUA.

[10] Goldberg I., 2006 *University of Waterloo - 7^{th} Annual Privacy and Security Workshop & 15^{th} CACR Information Security Workshop*

[11] crypto.stackexchange.com (2011) *What is the "Random Oracle Model" and why is it controversial? http://crypto.stackexchange.com/questions/879/what-is-the-random-oracle-model-and-why-is-it-controversial* Resposta escrita por *Thomas Pornin (bolet.org/ pornin).* Acesso em 18/10/14.

[12] J. Katz, A. Thiruvengadam e H.-S. Zhou (2013) *Feasibility and infeasibility of adaptively secure fully homomorphic encryption* Em *Proceedings of PKC 2013, LNCS 7778, 2013, pp.14–31*

[13] en.wikipedia.org (2014), *Diffie-Hellman_key_exchange - http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange Acesso em 01/12/2014*

[14] A Fiat, M Naor (1993) *Broadcast Encryption - Advances in Cryptology—CRYPTO'93, 1994 - Springer*

[15] Rodrigues, P M (2012) *Teorema Chinês do Resto - Notas de aula - O teorema chinês dos restos, Universidade de Lisboa, 2012*

[16] M. Di Raimondo, R. Gennaro, e H. Krawczyk (2005) *Secure Off-the-Record Messaging - WPES'05: Proceedings of the 2005 ACM workshop on Privacy in electronic society, paginas 81–89, New York, NY, USA, 2005. ACM.*

[17] Crypto Cat blog (2014) *https://blog.crypto.cat/2014/01/mpotr-project-plan/* - Postagem escrita por *Nadim*, acessada em 20/10/14.

[18] A. Shamir, (1985) *Identity-based cryptosystems and signature schemes - In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985*

[19] A. Sahai and B. Waters, (2005) *Fuzzy Identity-Based Encryption - Advances in Cryptology – EUROCRYPT 2005, pp 457-473*

[20] Chase, M. (2007) *Multi-authority Attribute Based Encryption - Theory of Cryptography, vol. 4392, Springer Berlin Heidelberg, pp. 515-534*

[21] J. Bethencourt, A. Sahai, and B. Waters (2007) *Ciphertext-policy attribute-based encryption - IEEE Symposium on Security and Privacy, 2007,pp. 321–334*

[22] Waters B. (2008) *Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization* - Cryptology ePrint Archive, Report 2008/290

[23] Lin, H., Cao, Z., Liang, X., Shao, J. (2008) *Secure threshold multi authority attribute based encryption without a central authority - In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 426–436. Springer, Heidelberg (2008)*

[24] A Lewko, B Waters (2011) *Decentralizing attribute-based encryption - Advances in Cryptology–EUROCRYPT 2011, Springer*

[25] Z. Liu, Z. Cao, Q. Huang, D.S. Wong e T.H. Yuen (2011) *Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption without Random Oracles - Proc. 16th European Symp. Research in Computer Security (ESORICS ',11), V. Atluri and C. Diaz, eds., pp. 278-297, Sept. 2011*

[26] M. Chase e S.S. Chow (2009) *Improving Privacy and Security in Multi-Authority Attribute-Based Encryption - Proc. ACM Conf. Computer and Comm. Security (CCS ',09), E. Al-Shaer, S. Jha, and A.D. Keromytis, eds., pp. 121-130, Nov. 2009*

[27] Jinguang Han and Susilo, W. and Yi Mu and Jun Yan (2012) *Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption, Parallel and*

Distributed Systems, IEEE Transactions on, 11 de novembro de 2012, pp. 2150-2162

[28] Pereira, H. V. L. (2013) *Um sistema de criptografia de broadcast para navegadores de internet - Depósito de TCCs - IME USP - http://bcc.ime.usp.br/principal/index.php?id=deposito-de-tccs Acesso em 01/09/2014*

[29] HUANG, Q., MA, Z., YANG, Y., FU, J., & NIU, X. (2014) *Secure Data Sharing and Retrieval Using Attribute-Based Encryption in Cloud-Based OSNs - Chinese Journal of Electronics, 23(3)*

[30] Canetti R., Feige U., Goldreich O., and Naor M. (1996) *Adaptively secure multi-party computation.* Em *28º Simposio anual ACM de teoria da computação (STOC), páginas 639–648. Editora ACM, 1996*