

Universidade Federal de São Carlos – UFSCar
Departamento de Computação – DC
Programa de Pós Graduação em Ciência da Computação – PPGCC
Grupo de Sistemas Distribuídos e Redes – GSDR
Tópicos em Sistemas Distribuídos: Privacidade e Personalização

O Jantar dos Criptógrafos

Docente: Prof. Dr. Sergio Donizetti Zorzo
Discente: Cláudio Rodolfo Sousa de Oliveira

Estrutura da Apresentação

- Introdução
- Uma abordagem Geral
- Modelo
- Exemplos
- Conspiração dos Participantes
- Técnicas de comunicação
- Relação com o Mix-net
- Desvantagens
- Aplicações Práticas
- Conclusão
- Bibliografia

Visão Geral

- Criptografia é o estudo dos princípios e técnicas pelas quais uma informação pode ser transformada da sua forma original para outra ilegível, e lida posteriormente pelo receptor.
- Criptógrafos são pessoas envolvidas no trabalho de criptografia em geral.
- Protocolos de criptografia são projetados para fornecer garantias de segurança de vários tipos usando mecanismos de criptografia:
 - ❖ Confidência, integridade de mensagem, autenticação, não repúdio, garantias de anonimato.

Visão Geral (cont.)

- Uma das tecnologias existentes de melhoria da privacidade para proteção da identidade do usuário (anonimato).
- Transmissor e receptor são, incondicionalmente, não localizáveis.
- Proteção em nível de Comunicação.
- Dining Cryptographers Net
 - ❖ Mensagens de difusão seguras (irreal),
 - ❖ Cada mensagem de difusão é recebida por todos os outros participantes sem ser modificada (participantes honestos).
- Dining Cryptographers Plus Net
 - ❖ Mensagens de Difusão não seguras.

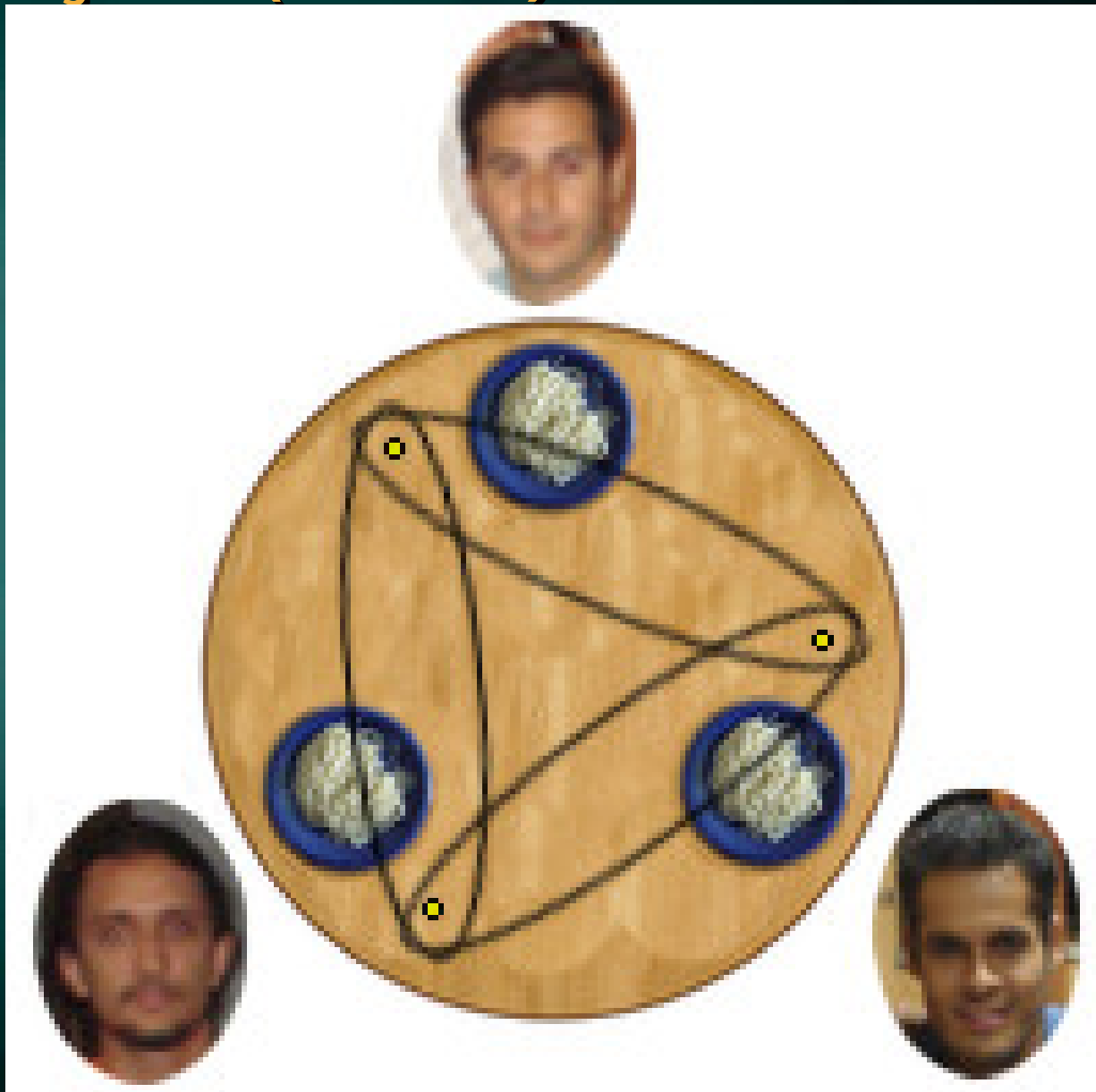
Resumo

- Parece impossível manter confidencial quem envia mensagens, em um mundo onde qualquer transmissão física pode ter sua origem localizada.
- O DC-net e o DC+-net fornecem uma total segurança por meios criptográficos utilizando a PKI (Public Key Infrastructure).
- Pode ser adaptado para ser utilizado em uma larga variedade de considerações práticas.

Introdução

- Três criptógrafos estão sentados para jantar no restaurante.
- O garçom os informa que o acordo foi feito com o maitre do hotel para a conta a ser paga anonimamente.
- Um dos criptógrafos poderia estar pagando pelo jantar, ou a NSA (a Agência de Segurança Nacional dos EUA), o empregador deles.
- O jantar só é pago uma vez.
- Os criptógrafos respeitam o direito dos outros realizarem um pagamento anônimo, mas se a NSA estiver pagando eles desejam saber.

Introdução (cont.)



Introdução (cont.)

- Eles solucionam sua incerteza de forma razoável através do seguinte protocolo:
 - ❖ Cada criptógrafo lança uma moeda atrás do seu cardápio, entre ele e o criptógrafo da sua direita, de forma que só os dois vejam o resultado.
 - ❖ Cada criptógrafo declara em voz alta se as duas caíram do mesmo lado ou em lados diferentes.
 - ❖ Se um dos criptógrafos é o pagador, ele declara o oposto do que ele vê.
 - ❖ Um número ímpar de diferenças dito à mesa indica que um criptógrafo está pagando.
 - ❖ um número par de diferenças indica que a NSA está pagando.
 - ❖ Os criptógrafos não pagantes não aprendem nada sobre qual dos outros dois é o pagante.

Introdução (cont.)

A	B	C
Ca	Ca	Ca
Ca	Ca	Co
Ca	Co	Ca
Ca	Co	Co
Co	Ca	Ca
Co	Ca	Co
Co	Co	Ca
Co	Co	Co

NSA Pagando		
A	B	C
I	I	I
D	I	D
I	D	D
D	D	I
D	D	I
I	D	D
D	I	D
I	I	I

A Pagando		
A	B	C
D	I	I
I	I	D
D	D	D
I	D	I
I	D	I
D	D	D
I	I	D
D	I	I

B Pagando		
A	B	C
I	D	I
D	D	D
I	I	D
D	I	I
D	I	I
I	I	D
D	D	D
I	D	I

C Pagando		
A	B	C
I	I	D
D	I	I
I	D	I
D	D	D
D	D	D
I	D	I
D	I	I
I	I	D

Introdução (cont.)

- O protocolo é totalmente seguro se for realizado fielmente.
- Considere um criptógrafo não pagador que deseja saber quem é o criptógrafo pagador.
- Se o NSA paga, não há problema de anonimato.
- Em um caso as moedas vistas são iguais, um dos outros disse "diferente", e o outro "igual."
 - ❖ Se o resultado escondido fosse igual aos dois resultados que ele vê, o criptógrafo que disse "diferente" é o pagador;
 - ❖ Se o resultado fosse diferente, o que disse, "igual" é o pagador.
- Nada pode ser afirmado. Existem apenas suposições.

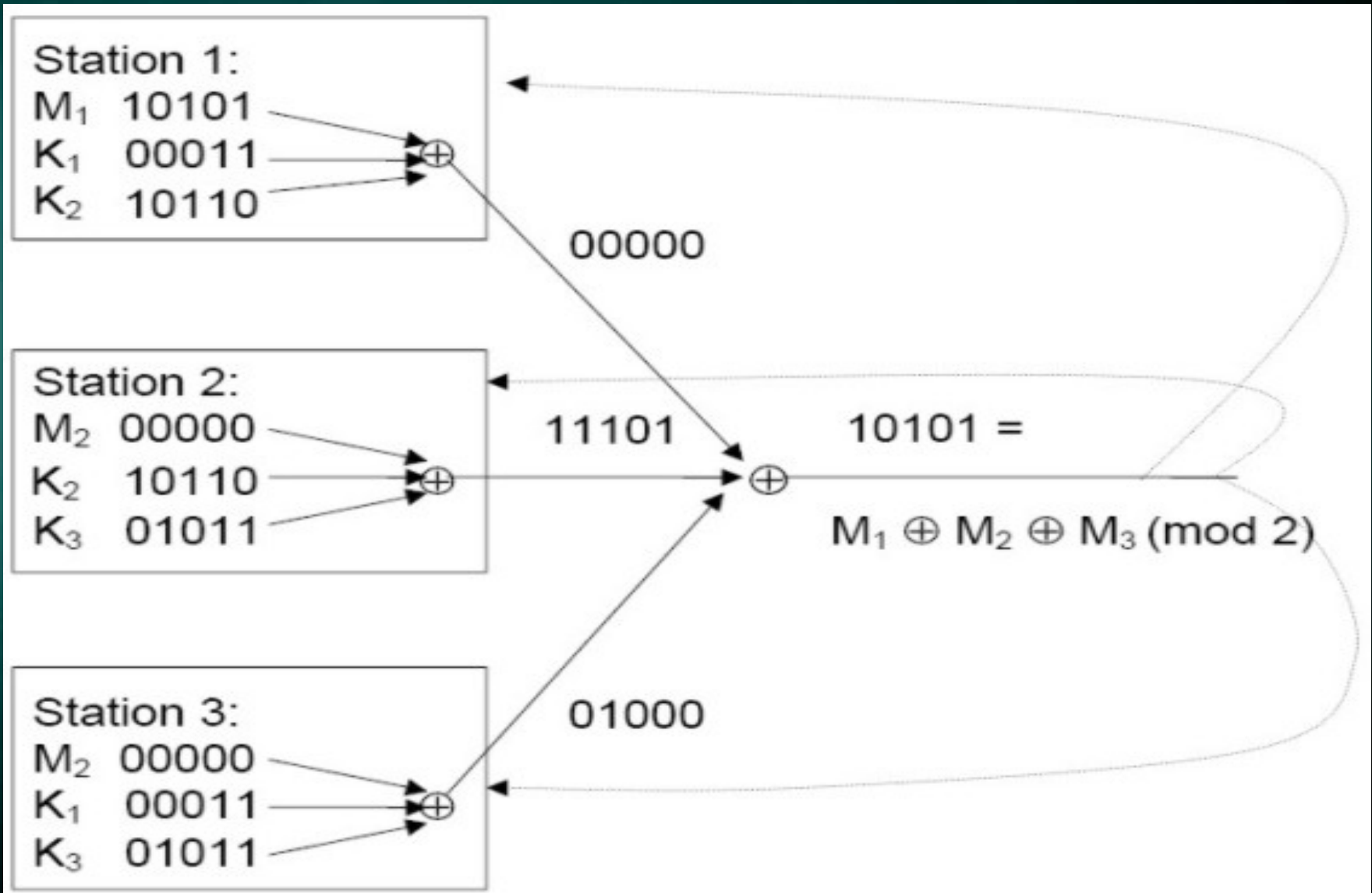
Introdução (cont.)

- **Caso (2) as moedas que ele vê são diferentes;**
 - ❖ Se ambos criptógrafos disseram "diferente", então o pagador está ao lado da moeda que é idêntica à moeda escondida;
 - ❖ Se ambos disseram "igual", então o pagador está ao lado da moeda que é diferente da moeda escondida;

Introdução (cont.)

- Os criptógrafos inventaram um modo de criar mensagens públicas sem pista à mesa para uma mensagem de qualquer tamanho.
 - ❖ o protocolo básico é repetido sucessivamente;
 - ❖ quando um criptógrafo deseja criar uma mensagem pública, ele começa a inverter suas declarações naquela rodada correspondente, em uma versão binária de sua mensagem codificada.
 - ❖ Se ele nota que a mensagem colidiu (detectada pelos transmissores porque a mensagem chegou diferente da enviada) com alguma outra, ele pode, por exemplo, esperar um número de rodadas aleatório antes de tentar transmitir novamente

Envio sobreposto por difusão



Envio sobreposto por difusão (cont.)

- Todos criptógrafos escolhem um número aleatório (0 ou 1) privadamente e o mostra para o criptógrafo a sua direita.
- Cada criptógrafo computa o x-or (subtração) entre seu número e o número que a ele foi mostrado pelo criptógrafo a sua esquerda, somando a mensagem se ele quiser transmitir.
- Ele anuncia o resultado publicamente.
- Todos os criptógrafos somam os números publicados.
- Se a soma é 0, ninguém enviou uma mensagem.

Envio sobreposto por difusão (cont.)

- Se a soma é uma mensagem válida, um criptógrafo transmitiu uma mensagem.
- Se a soma é inválida, mais de um criptógrafo tentou transmitir uma mensagem (houve colisão).
- O anonimato do receptor:
 - ❖ Todo o mundo recebe a mensagem ao mesmo tempo, assim a mensagem poderia ser para qualquer um.
- O anonimato do transmissor:
 - ❖ seguro porque ninguém conhece as chaves outros participantes (somente da pessoa a sua direita, quando não há conspiração)
- Para dois criptógrafos, não há anonimato.

Uma abordagem Geral

- Durante o jantar, os criptógrafos consideram também um número de participantes maior que pode realizar uma versão do protocolo.
- Cada participante produz a soma do módulo dois, de todos os bits da chave que ele compartilha e se ele desejar transmitir, ele inverte sua produção.
- Se nenhum participante transmite, a soma do módulo dois das produções deve ser zero.
- Se um participante transmite, a soma deve ser um.

Modelo

- Cada participante tem duas informações secretas:
 - ❖ (a) as chaves compartilhadas com os outros participantes em cada rodada;
 - ❖ (b) a inversão usada em cada rodada (i.e., 1 se o participante inverte naquele rodada e 0 se não).
- Alguns ou todos os segredos do participante podem ser dados aos outros participantes em várias formas de conspiração.
- A possibilidade de segredos serem roubados é ignorada até por enquanto.

Modelo (cont.)

- As informações públicas do sistema são:
 - ❖ (a) quem compartilha chaves com quem;
 - ❖ (b) o que cada participante resulta durante cada rodada (a soma do modulo dois das chaves do participante e a inversão).
- Estas informações não precisam ser secretas para assegurar a não localização.
- A soma de todos os resultados, se tornará conhecida por todos os participantes.

Modelo (cont.)

- Na terminologia de grafos, cada participante corresponde a um vértice e cada chave corresponde a uma aresta.
- Uma aresta é incidente nos vértices que corresponde ao par de participantes que compartilham a chave correspondente.
- Também será assumido que o grafo está conectado.

Exemplos

- Se todos os participantes cooperam completamente contra um, claro que o protocolo não pode manter as mensagens deste único sem pistas.
- A não localização só existe entre um conjunto de possíveis atores (conjunto de anonimato).
- Se um conjunto tem somente um membro, suas mensagens são localizáveis.
- Cada participante agindo só nada aprende sobre a contribuição de outros participantes.

Conspiração dos Participantes

- Alguns participantes podem cooperar agrupando suas chaves em esforços para localizar as mensagens dos outros;
- Tal cooperação é chamada conspiração.
- Para simplicidade, as possibilidades de múltiplas conspirações ou de agrupamento de outras informações que completa as aresta (chaves) serão ignoradas.

Conspiração dos Participantes (cont.)

- Os membros de uma conspiração completa
 - ❖ tem um conjunto com todas as chaves.
- Os membros de uma conspiração parcial
 - ❖ agrupam algumas mas não todas as suas chaves.
- Conspiradores podem unir uma conspiração (parcial) sem ter que se fazer completamente localizáveis para os outros membros da conspiração.

Estabelecendo Chaves

- Para fornecer chaves para mensagens mais longas, cada membro deve lançar muitas moedas com antecedência.
- Os bits resultantes são armazenados em disco.
- Se os participantes não transmitem o tempo todo, as chaves podem ser criadas usando uma taxa mais lenta quando nenhuma mensagem está sendo enviada;
- a taxa completa retornaria automaticamente só quando uma mensagem fosse ser transmitida.

Estabelecendo Chaves (cont.)

- Outra possibilidade é estabelecer uma curta chave e usar um gerador de seqüência criptográfica pseudo-aleatório para ampliar isto assim que necessário.
- Claro que este sistema poderia ser quebrado se o gerador fosse quebrado.
- Até mesmo quando os criptógrafos não trocam as chaves no jantar, eles podem fazer seguramente depois usando um sistema de distribuição de chaves públicas.

Técnicas de Comunicação

- Diversos tipos de redes de comunicação podem ser usadas, e a topologia delas não importa para o protocolo.
- Sistemas de comunicação baseado em anéis são comuns em redes locais.
- Em um anel típico, cada nodo recebe cada bit e o passa na rede em round-robin para o próximo nodo.
- Esta tecnologia é prontamente adaptada para o presente protocolo.

Técnicas de Comunicação (cont.)

- Considere uma mensagem de único bit como "paguei".
- Cada participante faz o ou-exclusivo do bit que ele recebe com o próprio resultado dele antes de enviá-lo ao próximo participante.
- Quando o bit passou pela rodada completa, o ou-exclusivo é a soma dos resultados de todos os participantes, que é o resultado desejado do protocolo.

Técnicas de Comunicação (cont.)

- colisões são descobertas somente depois das transmissões de bits (demoradas), no qual só depois disso que pode conhecer os resultados de um rodada.
- Em sistemas de difusão o uso mais eficiente da capacidade do canal é obtido agrupando-se o resultado do participante em um bloco de tamanho de uma mensagem.

Técnicas de envio

● Mapa de reserva

- ❖ Em uma rede com muitas mensagens por bloco, um primeiro bloco pode ser usado por vários transmissores anônimos para pedir uma "reserva de slot" em um outro bloco.
- ❖ Quando há mais de uma reserva por slot haverá colisão.
- ❖ Evita colisão de mensagens.

● Slotted ALOHA

- ❖ Simplesmente espera-se o próximo slot para transmitir.
- ❖ Maior taxa de colisão.

Segredo e Autenticação

- Um criptógrafo pode assegurar o segredo de uma mensagem anônima por codificação da mensagem com a chave de pública do receptor.
- O transmissor pode manter até mesmo a identidade do receptor em segredo deixando todos os receptores tentarem decifrar a mensagem.
- Um prefixo (pseudo-endereço) poderia ser ligado a cada mensagem de forma que o receptor precise somente decifrar mensagens com prefixos endereçados a ele.
- Pode se modificar os prefixos cada vez que uma mensagem é transmitida.

Segredo e Autenticação (cont.)

- Poderiam ser concordados prefixos novos com antecedência, gerados criptograficamente quando necessário, ou fornecido em mensagens anteriores.
- Embora as mensagens sejam sem pista, eles ainda poderiam suportar assinaturas digitais.
- Só o dono não localizável seria capaz de enviar mensagens subseqüentes desta forma.
- Protocolos de pagamento seguros têm sido propostos no qual o pagador e/ou beneficiário poderia ser não localizáveis.
- Foram propostos outros protocolos que permitem indivíduos conhecidos apenas por pseudônimos transferir informações.

Localizando por Consentimento

- O uso anti-social de uma rede pode ser intimidado se a cooperação da maioria dos participantes torna isto possível, embora custoso, localizar qualquer mensagem.
- Se uma mensagem ameaçadora é enviada, um tribunal poderia ordenar que todos os participantes revelassem os seus bits chave compartilhados para uma rodada da mensagem.
- O transmissor da mensagem ofensiva poderia tentar espalhar a culpa, porém, mentindo sobre algum bits compartilhados.
- Assinaturas Digitais podem ser usadas para parar completamente a propagação da culpa.

Relação com o Mix-net

- Há um protocolo seguro de transmissão sem pistas, chamado Mix-net.
- O Mix-net confia na segurança de um sistema de chaves públicas.
- O DC-net pode usar a distribuição de chave pública para fornecer um sistema seguro.
- Num ambiente onde há limitações de canais, o Mix-net pode operar e o DC-net não.
- Num ambiente onde há conspirações, o DC-net pode operar e o Mix-net não.

Relação com o Mix-net (cont.)

- Mix-net também podem fornecer transmissão sem pistas neste ambiente de comunicação, embora haja largura da banda insuficiente para uso da difusão.
- Se é fornecida uma ótima proteção contra conspiração e há segurança criptográfica, Mix-net é aceitável.

Relação com o Mix-net(cont.)

- Uma escolha entre Mix-net, e DC-net pode depender da natureza do tráfego.
 - ❖ Com um sistema como correio que requer somente entregas periódicas e onde há um grande número de mensagens por unidade de tempo, Mix-net é indicado.
 - ❖ Quando as mensagens devem ser entregues continuamente e não há nenhum tempo para criar grande blocos delas, DC-net é preferível.

DC+-net

- Não aumenta a complexidade do DC-net.
- Considera uma rede de comunicação que pode falhar (devido ao protocolo fail-stop).
 - ❖ O fail-stop para a transmissão de mensagens quando 2 participantes recebem chaves diferentes ou não as recebe.

Ataques ativos

- O atacante apenas observa a comunicação entre 2 participantes sem alterá-la.
- Localização de um participante X
 - ❖ A transmite uma mensagem M para X;
 - ❖ X responde a mensagem de A com outra M'
 - ❖ Se o atacante é capaz de identificar o Tx de M' ele sabe que é o receptor de M (o mesmo);
 - ❖ Da mesma forma pode identificar o transmissor de M.

Desvantagens do DC-net

- Sobrecarga do canal por envio de mensagens por difusão para cada receptor.
- Overhead no envio de mensagens.
 - ❖ Para enviar 1 bit para um grupo de N participantes é preciso de N bits aleatórios.
- Requer uma segurança no canal aos pares entre os membros do grupo
 - ❖ Necessário para compartilhar o bit chave.
- Transmissão lenta
 - ❖ Um bit por vez

Aplicações Práticas

The Free Haven Project (www.freehaven.net)

- [Molnar, David and Freedman, Michael (2007)]
 - ❖ Tem o objetivo de desenvolver um sistema distribuído, anônimo [...] e robusto contra tentativas de adversários encontrar e distribuir os dados armazenados, similar aos sistemas P2P atuais.
 - ❖ Considera uma possível implementação do DC-net para o projeto, de sistema anônimo.
 - ❖ A problemas de eficiência do protocolo e a dificuldade de implementação correta.
 - ❖ Numa possível implementação, usar apenas o DC-net não seria uma boa idéia.
 - ❖ Poderia considerar-se o uso do DC-net utilizando Mixes para esconder a identidade de cada participante.
 - ❖ Neste cenário enquanto um fracasso do Mix revelaria a identidade de um participante, a difusão anônima impediria de se ligar uma mensagem a um participante.

Dining Cryptographers Revisited

● [Golle and Juels (2004)]

- ❖ Chaum desenvolveu o Mix-net e o **DC-net** para prover transmissão anônima de mensagens.
- ❖ O Mix-net é amplamente discutido e serve como base para diversos sistemas de anonimato.
- ❖ Em contraste, o DC-net foi mantido **abandonado** aparecendo apenas em alguns artigos dispersos.

The dining cryptographers problem: unconditional sender and recipient untraceability

- [Chaum D. (1988)]

- ❖ O primeiro artigo sobre o DC-net e propõe o protocolo.
- ❖ Mostra a idéia geral do protocolo.

k-Anonymous Message Transmission

- [Ahn, Luis; Bortz, Andrew and Hopper, Nicholas. (2003)].
 - ❖ Descreve o funcionamento do **DC-net**, Mix-net and Onion Routing, Crowds e ClickNet, protocolos que serviram de base para este protocolo.
 - ❖ É um outro protocolo próprio.
 - ❖ É similar ao DC-net mas possui inovações
 - ❖ Considera-se k-grupos ou invés de um grupo.
 - ❖ Desvantagens citadas do DC-net : Não é adequado para uso em média ou larga escala.
 - ❖ Baixa escalabilidade.
 - ❖ Possui ordem de complexidade n^3 .

Detection of Disrupters in the DC Protocol

- [Bos, Jurjen; Boer, Bert. (1989)]
 - ❖ O Artigo foi encontrado apenas em <http://www.springerlink.com>
 - ❖ Valor \$ 25,00.
 - ❖ Trata do problema dos “interrompedores”, que são indivíduos que atrapalham ou impedem os outros de enviarem mensagens através de flooding o outro meio.
 - ❖ Encontrar disruptes é um problema de ordem quadrática.

The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability.

- [Waidner, Michael and Pfitzmann, Birgit. (1989)]
 - ❖ Jovens Criptográficos numa discoteca.
 - ❖ Problema: ruído.
 - ❖ Problema em uma consideração prática, mas sem implementação.

Unconditional Sender and Recipient Untraceability in spite of Active Attacks

- [Waidner, Michael (1989)]
 - ❖ Propõe o DC+-net, uma abordagem mais real do DC-net.
 - ❖ O DC+-net considera canal com ruído
 - ❖ Trata o problema de recebimento de mensagens errôneas.

Implementações

- [Meyden, Ron. (2003)] Symbolic Model Checking the Knowledge of the Dining Cryptographers
 - ❖ Mostra uma implementação algorítmica (não utiliza uma linguagem alvo) do protocolo DC-net.
- [Schneier, Bruce. (2005)] Cryptographic Ouija Board: CryptDining.
 - ❖ Implementação em Pearl do DC-net.
- [Storer. (2004)] Anonymity: An Explanation of the Dining Cryptographer's Algorithm.
 - ❖ Implementação em Java do DC-net.

Conclusão

- Esta solução para o problema do jantar dos criptógrafos mostra que um sistema de distribuição de chaves públicas pode ser usado para construir um canal computacionalmente seguro de transmissão não localizável.
- O DC-net é capaz de satisfazer uma gama extensiva de problemas práticos, onde envolvam o anonimato do transmissor ou/e receptor.
 - ❖ Voto digital anônimo, compra digital anônima, envio de e-mail anônimo.

Conclusão (cont.)

- Para um protocolo desenvolvido em 1988, se até 2003 é mantido abandonado, não teve nenhum importante impacto para a área.
- É uma especificação interessante, para uso em baixa escala.
- **Não há implementações práticas** do DC-net, sendo um protocolo utilizado apenas para fins didáticos.

Bibliografia

- Ahn, Luis; Bortz, Andrew and Hopper, Nicholas. (2003). “k-Anonymous Message Transmission”. In *Proc. of ACM CCS '03*, pp. 122-130. ACM Press.
- Bos, Jurjen; Boer, Bert. (1989). “Detection of Disrupters in the DC Protocol”. In *Proc. of Eurocrypt '89*, pp. 320-327. LNCS 434.
- Chaum David (1988). “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”. In *Journal of Cryptology*, 1(1), pp. 65-75.
- Golle, Philippe and Juels, Ari (2004). “Dining Cryptographers Revisited”. In J. Cachin and J. Camenisch, eds., *Eurocrypt '04*, pp. 456-473. Springer-Verlag. LNCS no. 3027 .

Bibliografia (cont.)

- Meyden, Ron and Su, Kaile. (2004). “Symbolic Model Checking the Knowledge of the Dining Cryptographers”. Computer Security Foundations Workshop. Proceedings. 17th IEEE. pp. 280 – 291.
- Molnar, David and Freedman , Michael (2007). “The Free Haven Project”. Computer Based Learning Unit, University of Leeds.
- Schneier, Bruce. (2005). “Cryptographic Ouija Board: CryptDining - The Dining Cryptographers' Protocol”.
- Storer, Tim. (2004). “Anonymity: An Explanation of the Dining Cryptographer’s Algorithm” pp 1-3.

Bibliografia (cont.)

- Waidner, Michael and Pfitzmann, Birgit. (1989). “The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability”. In *Proc. of Eurocrypt '89*, LNCS 434.
- Waidner, Michael (1989). “Unconditional Sender and Recipient Untraceability in spite of Active Attacks”. In *Proc. of Eurocrypt'89*, pp. 302-319. LNCS 434.