Introdução à Privacidade: Uma Abordagem Computacional

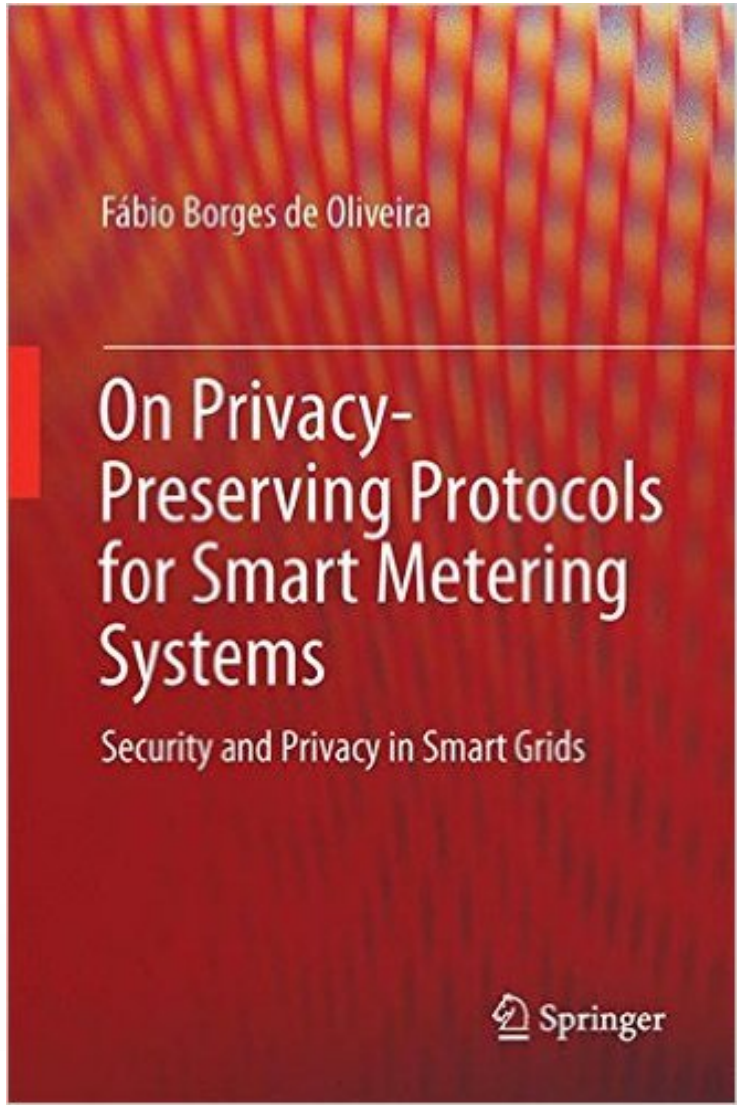
SBSeg 2016 - Minicurso

Prof. Dr.-Ing. Fábio Borges de Oliveira

Laboratório Nacional de Computação Científica (LNCC)
Coordenação de Sistemas e Redes (CSR)

Tópicos

O que é privacidade?



Direitos

Ninguém deverá ser submetido a interferências arbitrárias na sua vida privada, família, domicílio ou correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques todas as pessoas têm o direito à proteção da lei. [Artigo 12 da Declaração Universal dos Direitos Humanos de 1948]

[http://www.un.org/en/universal-declaration-human-rights/]

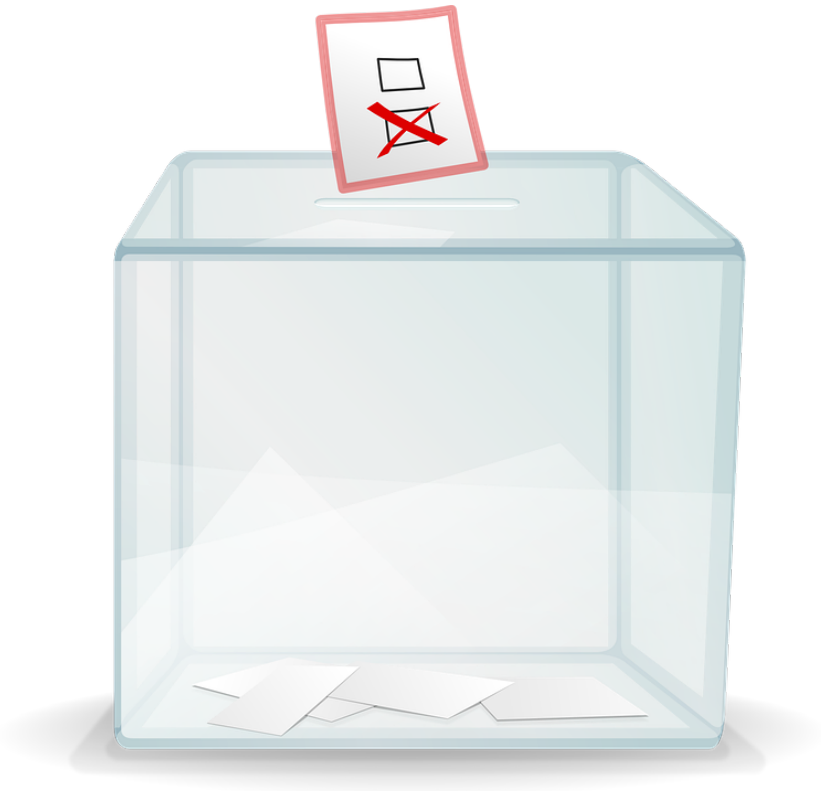
[http://www.humanrights.com/pt/what-are-human-rights/videos/right-to-privacy.html]

A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. [Art. 8º LEI brasileira Nº 12.965, DE 23 DE ABRIL DE 2014.]

Uma questão de escolha?

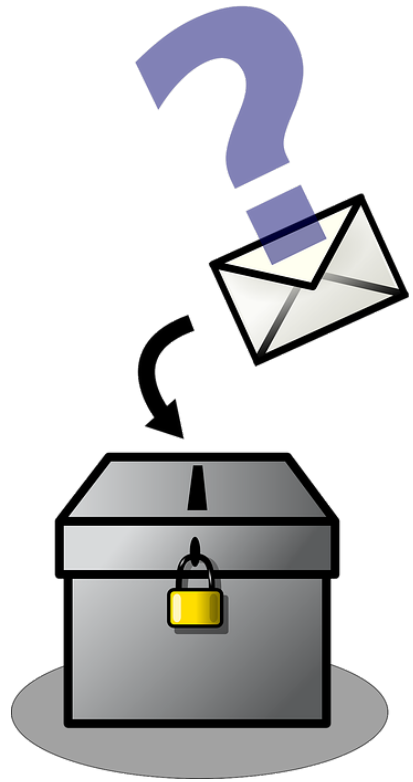
Votação Eletrônica [CGS97]

- Similar ao processo físico [Gri02]



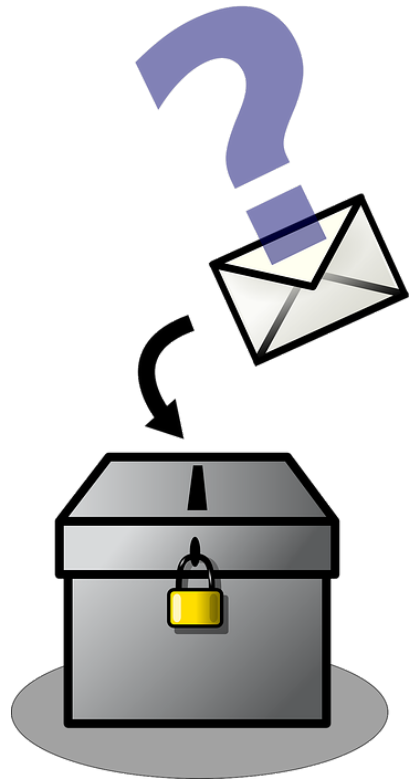
Votação Eletrônica [CGS97]

- Similar ao processo físico [Gri02]
- Voto secreto



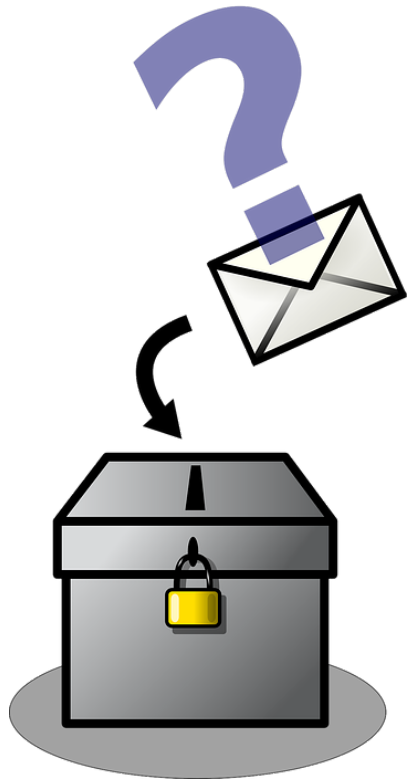
Votação Eletrônica [CGS97]

- Similar ao processo físico [Gri02]
- Voto secreto
- Verificabilidade [Gri02]



Votação Eletrônica [CGS97]

- Similar ao processo físico [Gri02]
- Voto secreto
- Verificabilidade [Gri02]
- Para evitar conflito, pode-se imprimir o voto

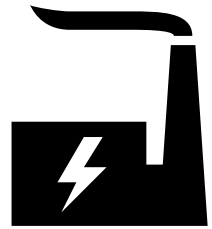


Sistemas de Reputação

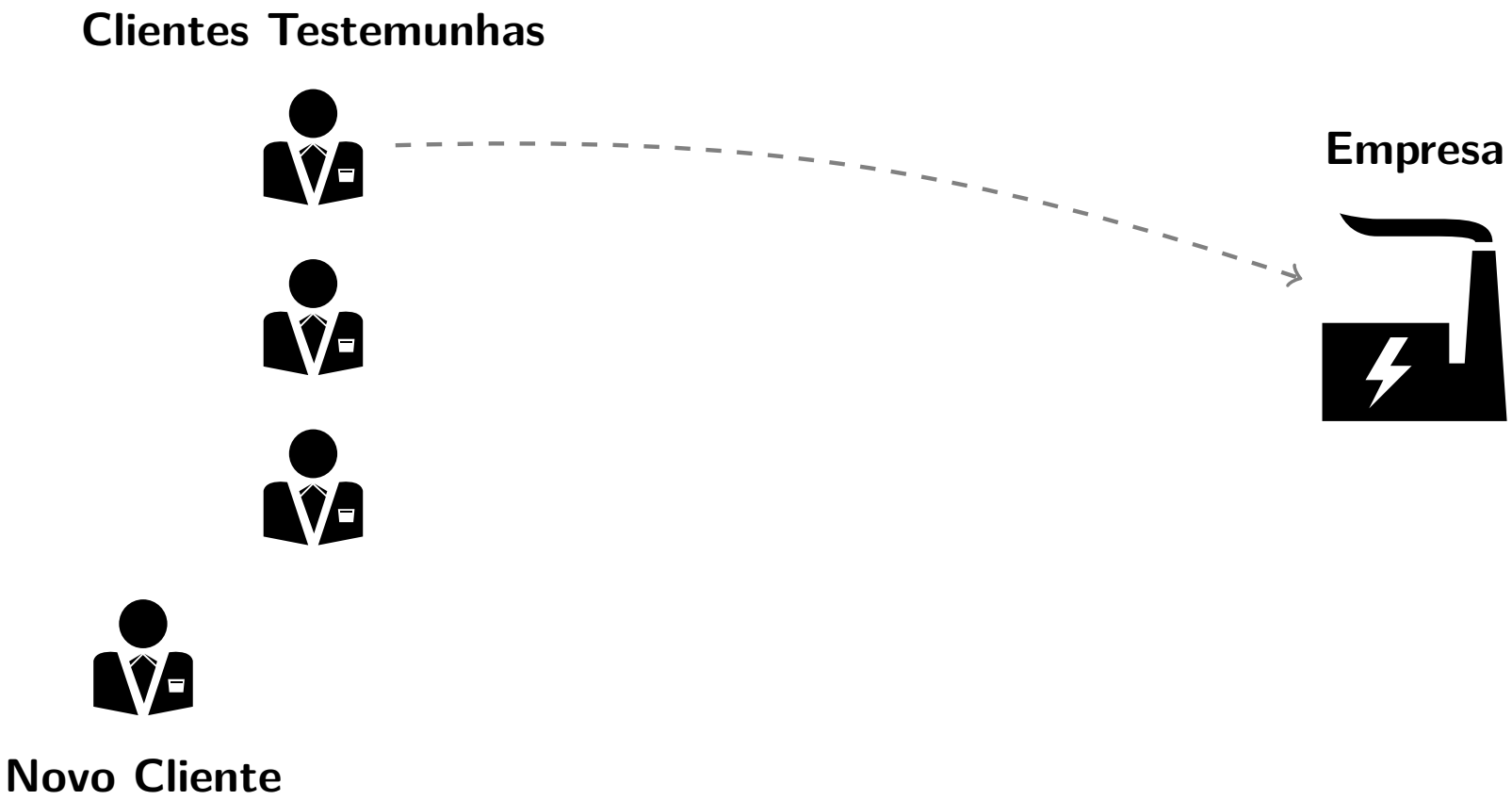
Clientes Testemunhas

Novo Cliente

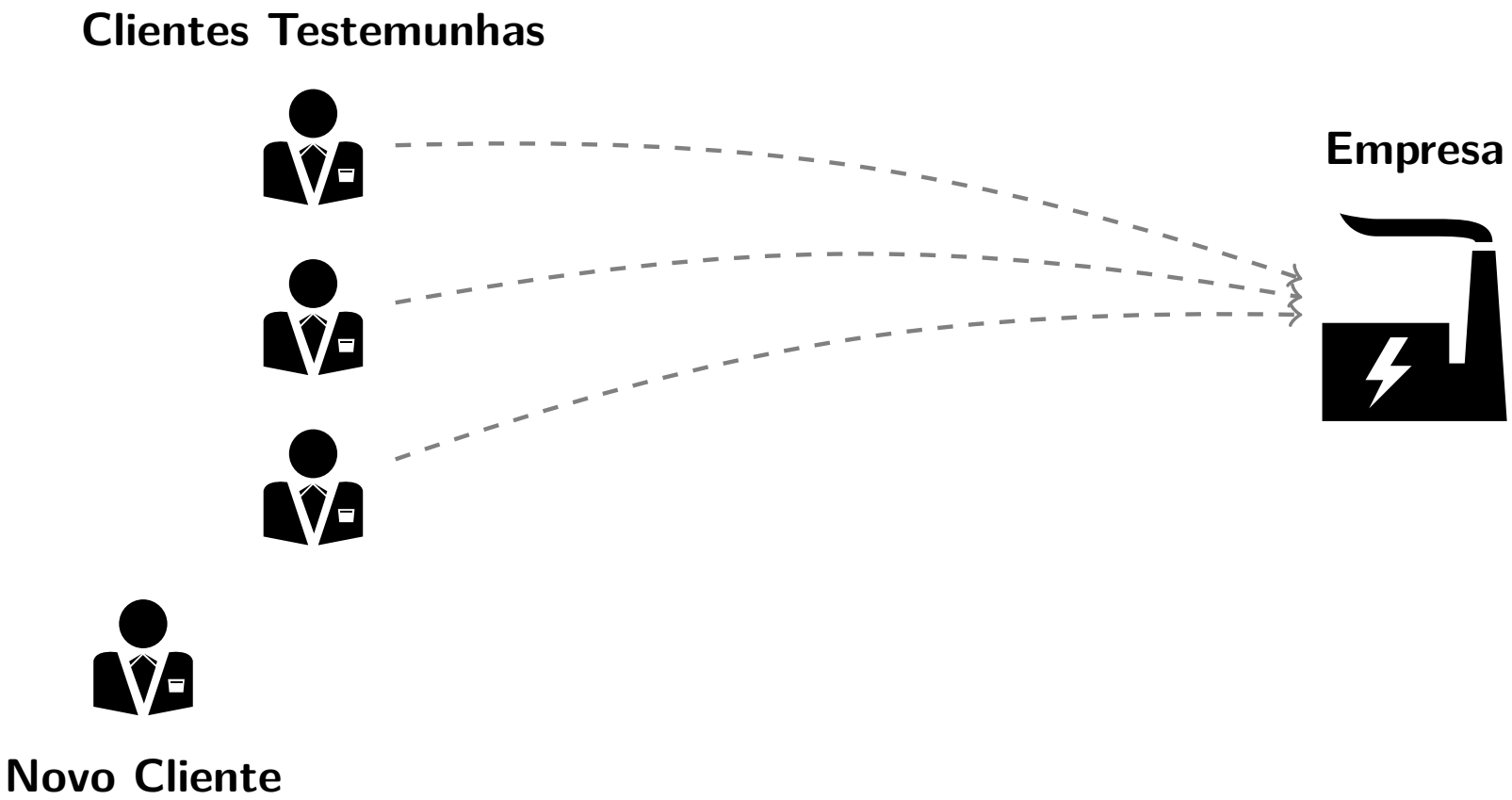
Empresa



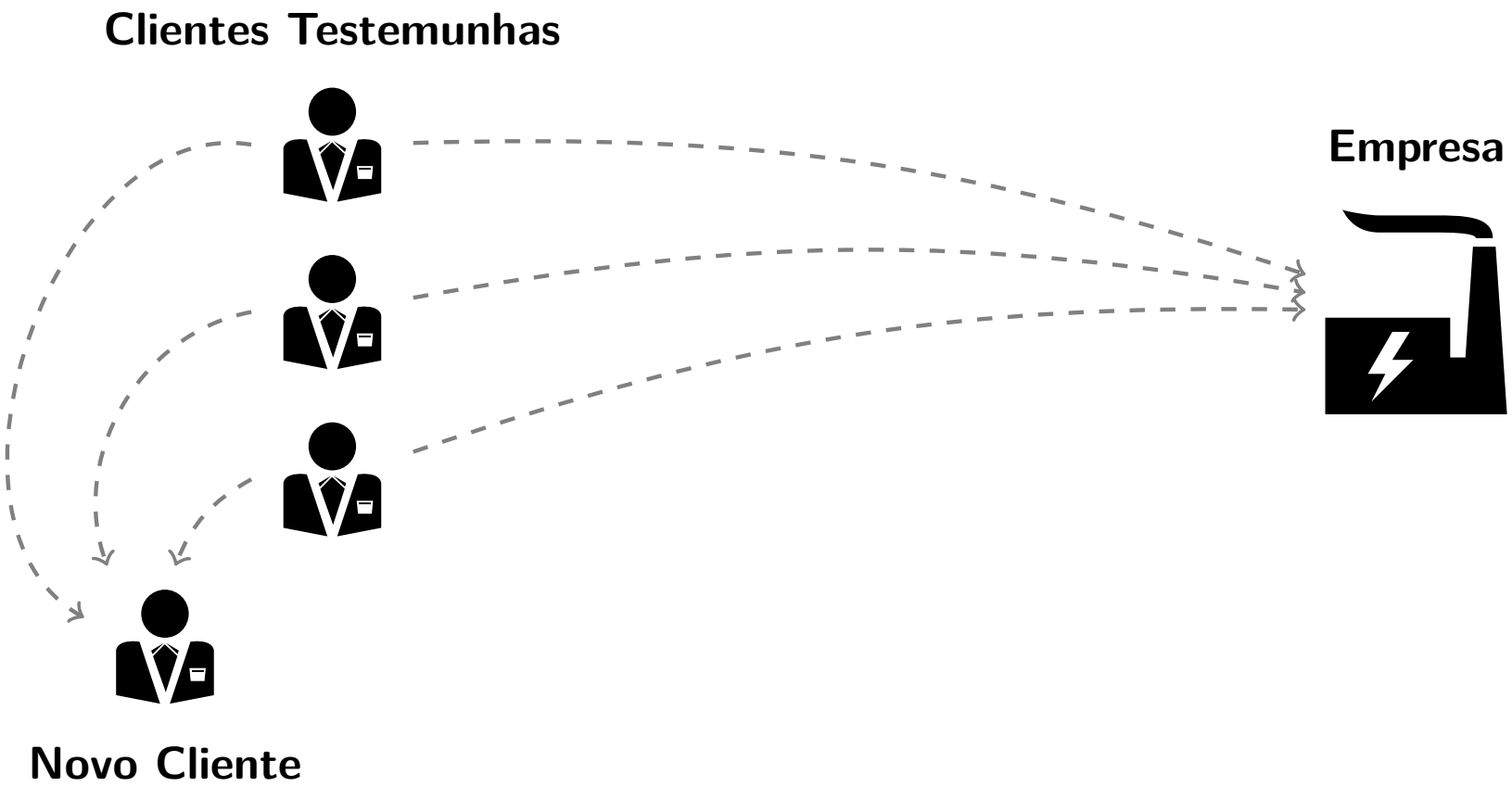
Sistemas de Reputação



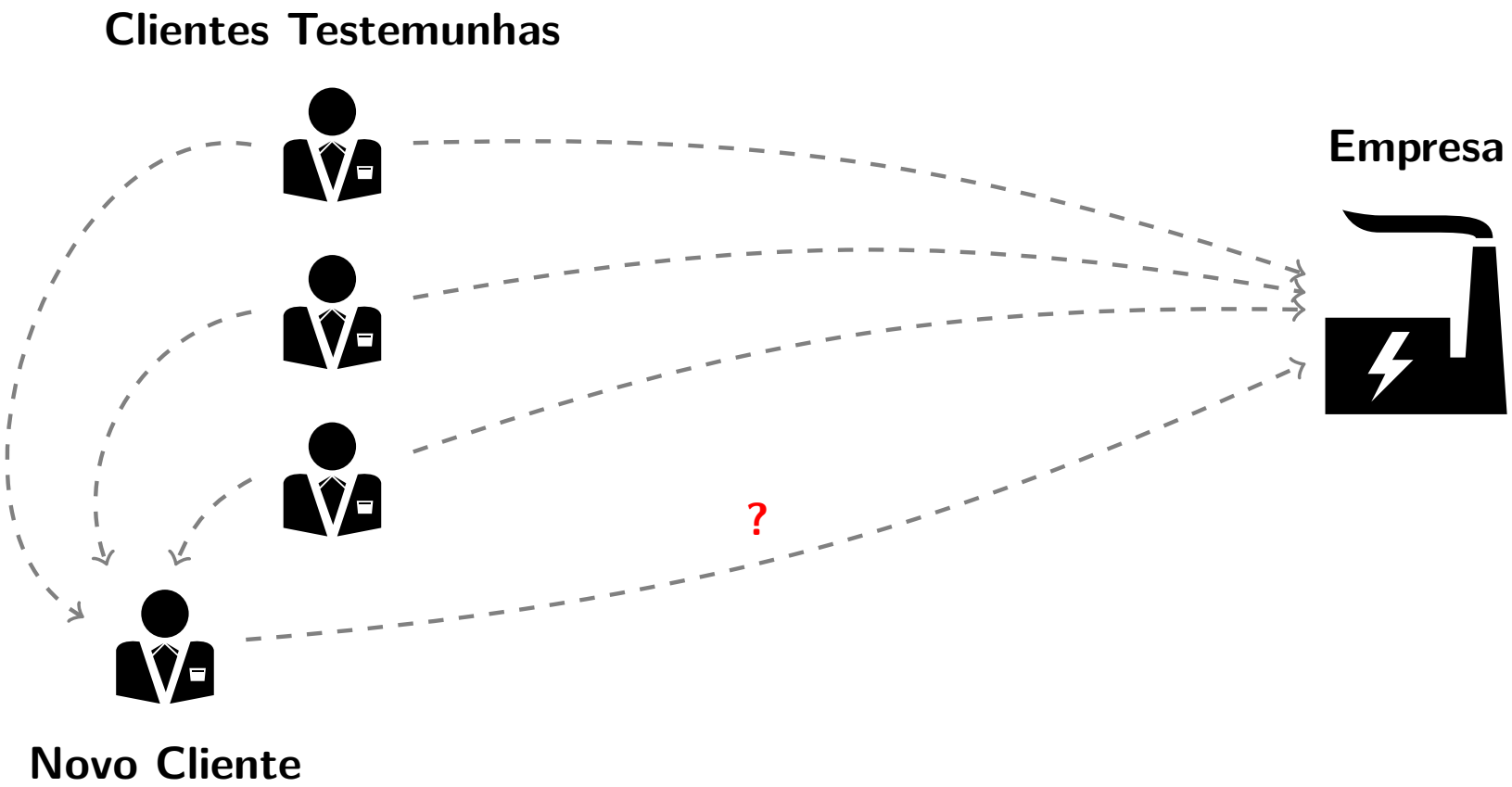
Sistemas de Reputação



Sistemas de Reputação

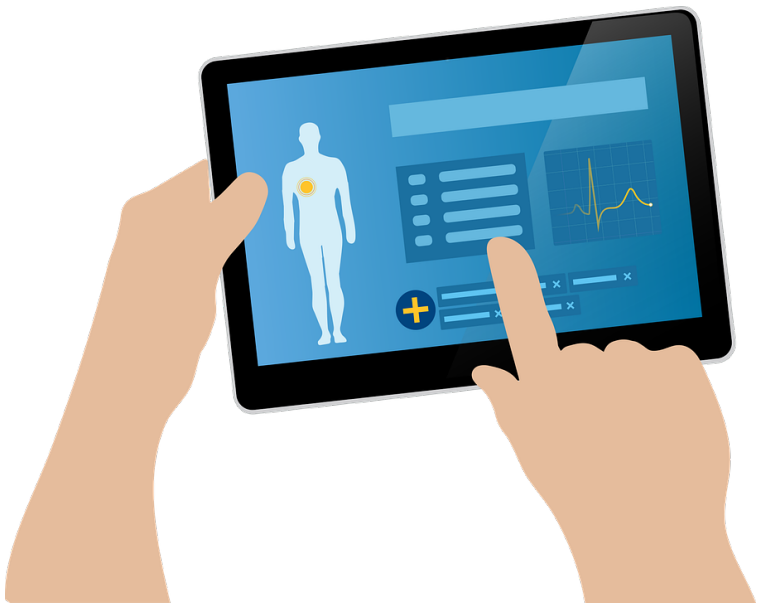


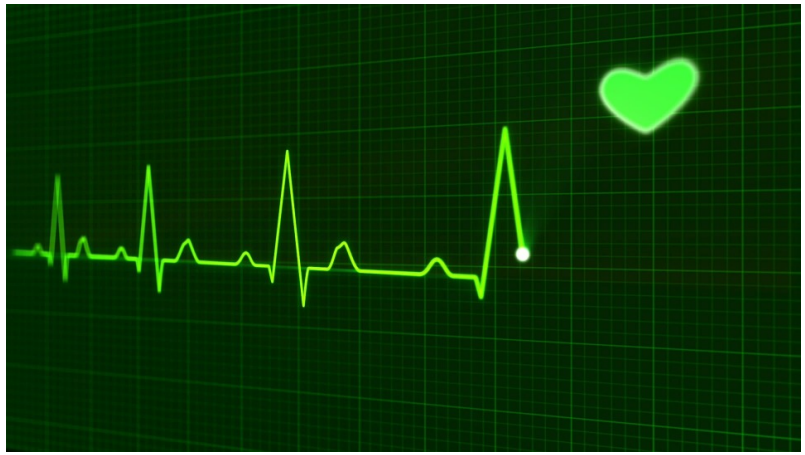
Sistemas de Reputação



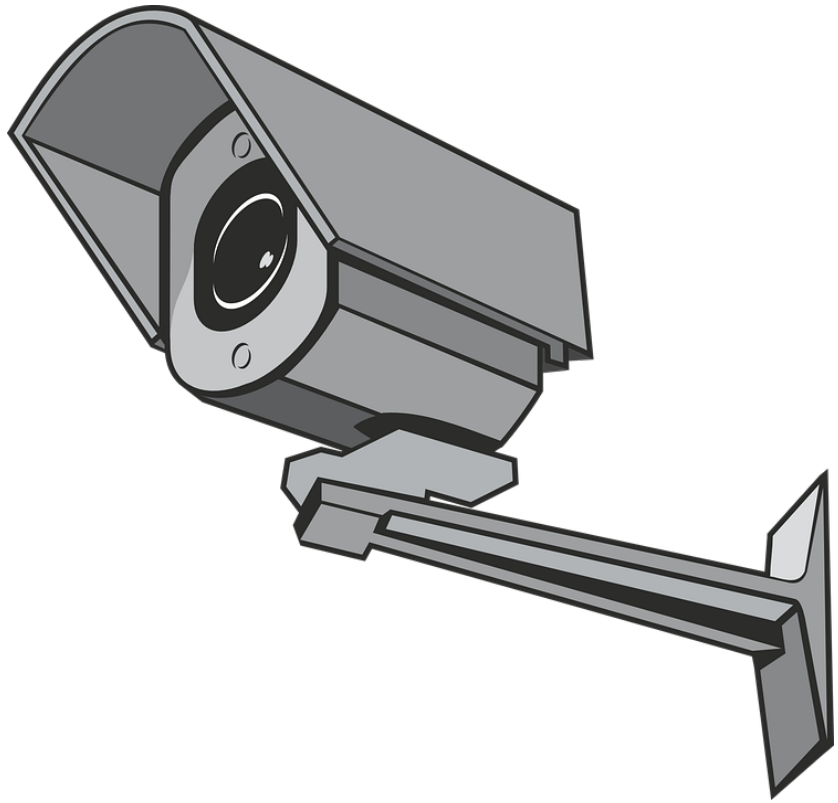
Redes de Sensores

Cibermedicina



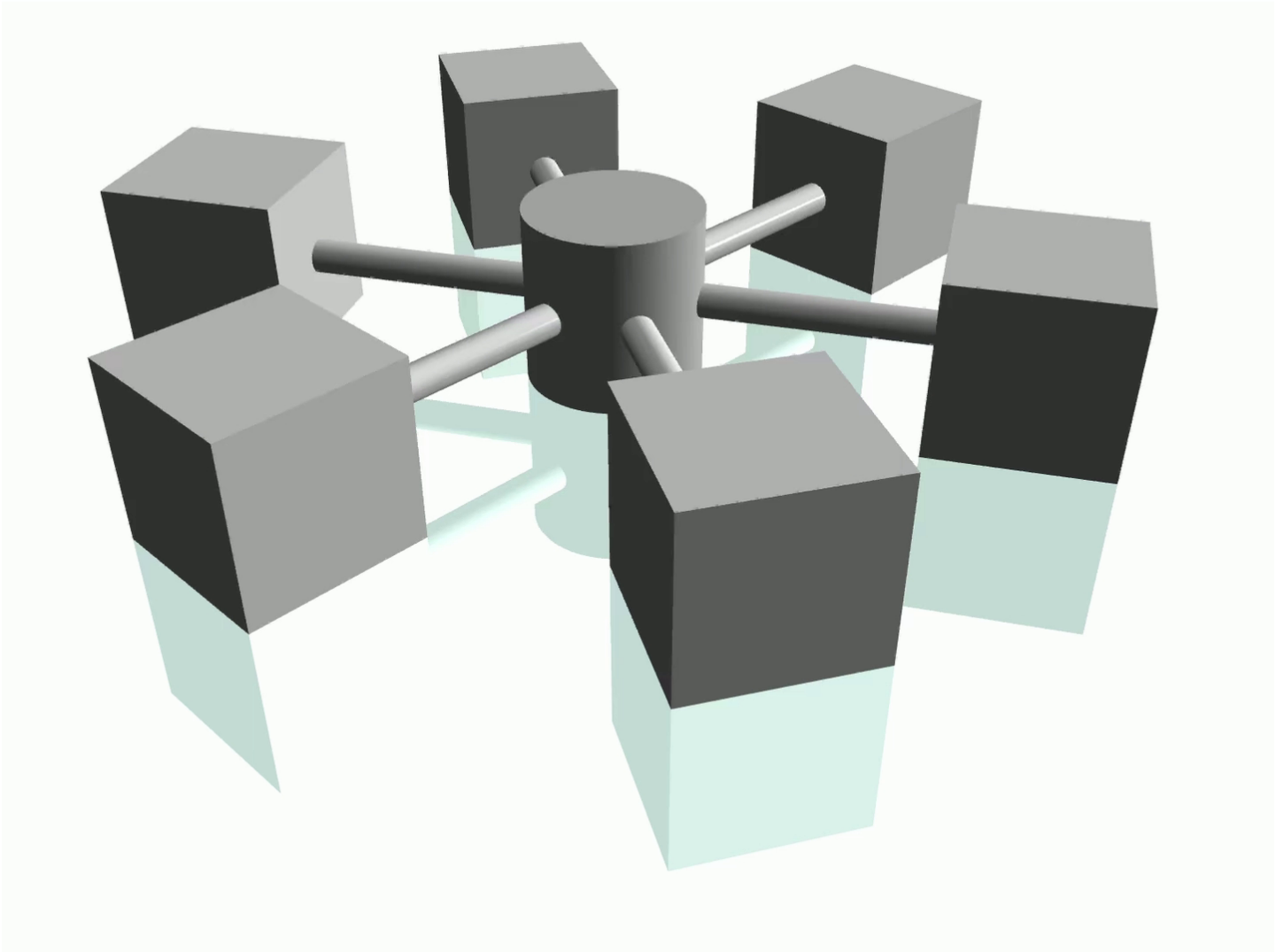


Processamento de Imagem

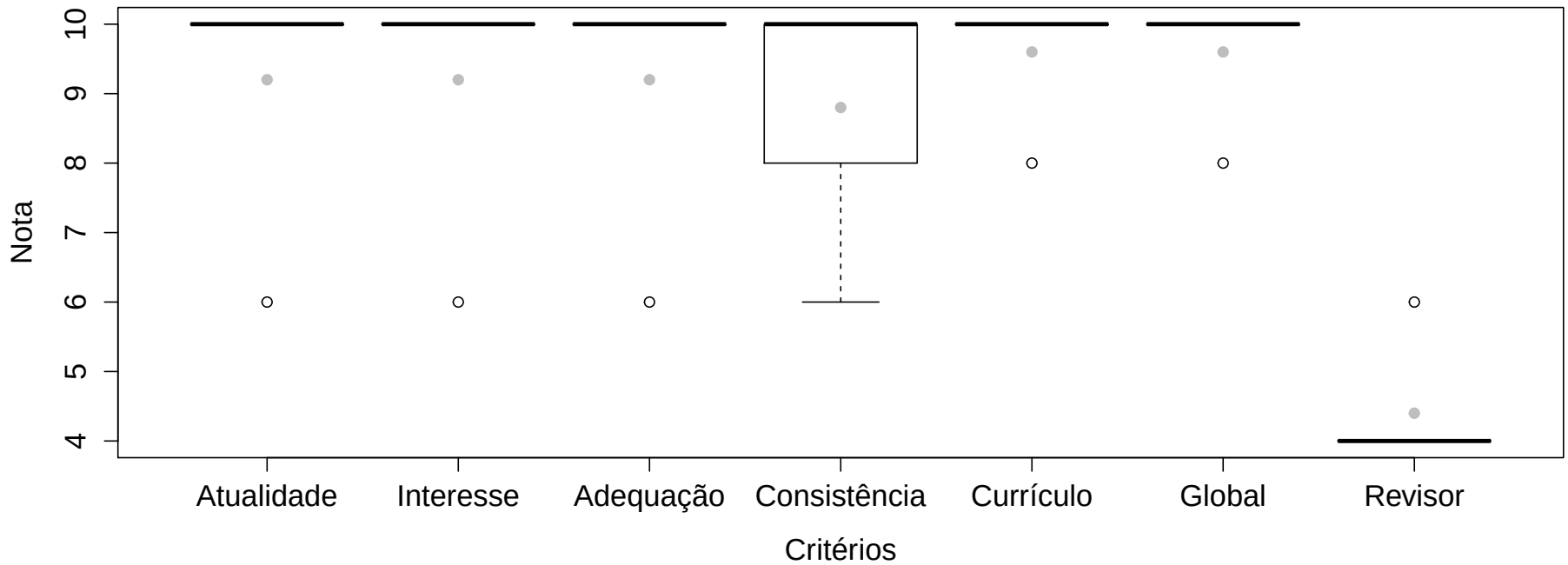


Dinheiro Eletrônico

Computação em Múltiplas Partes

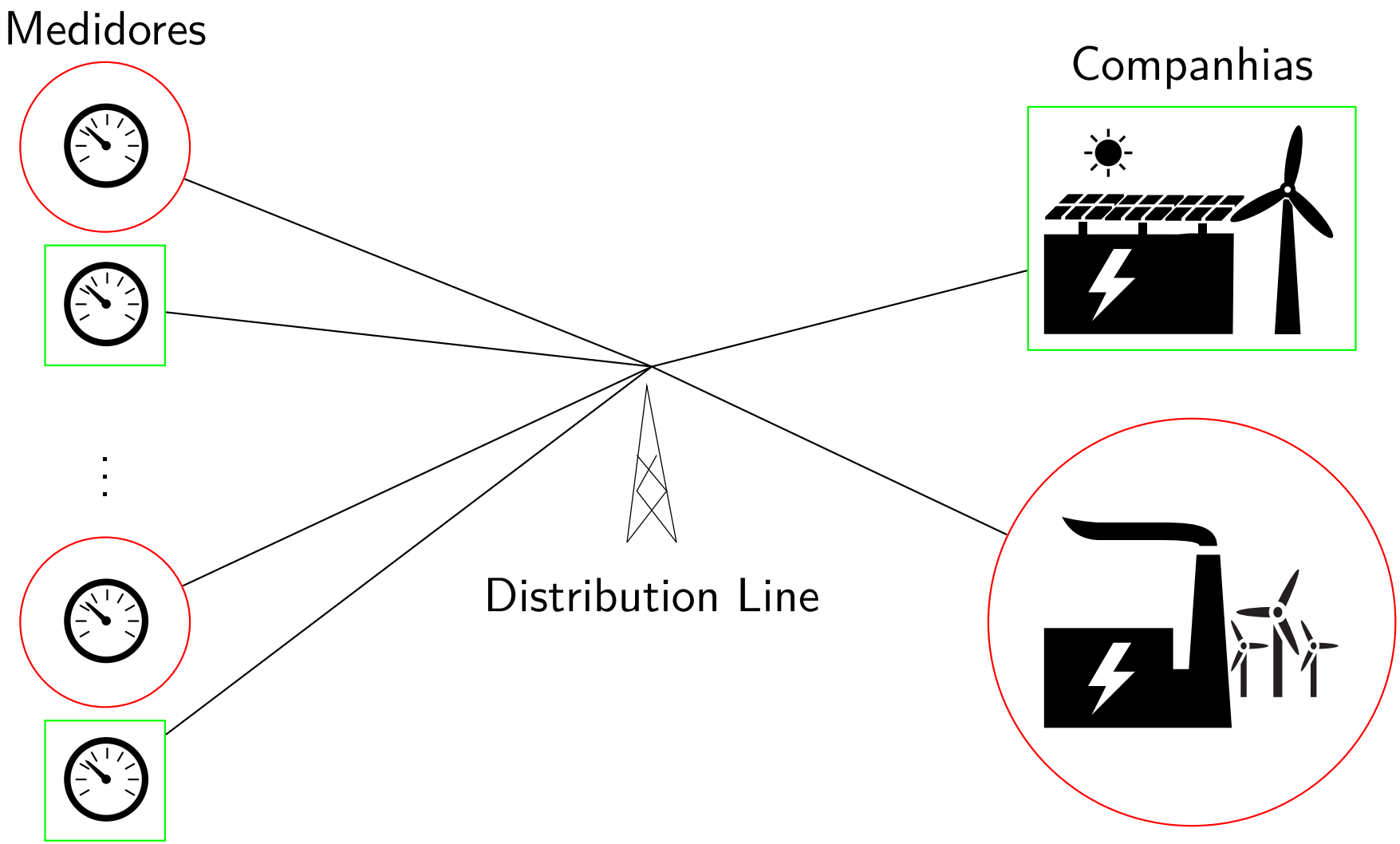


No Mundo Acadêmico



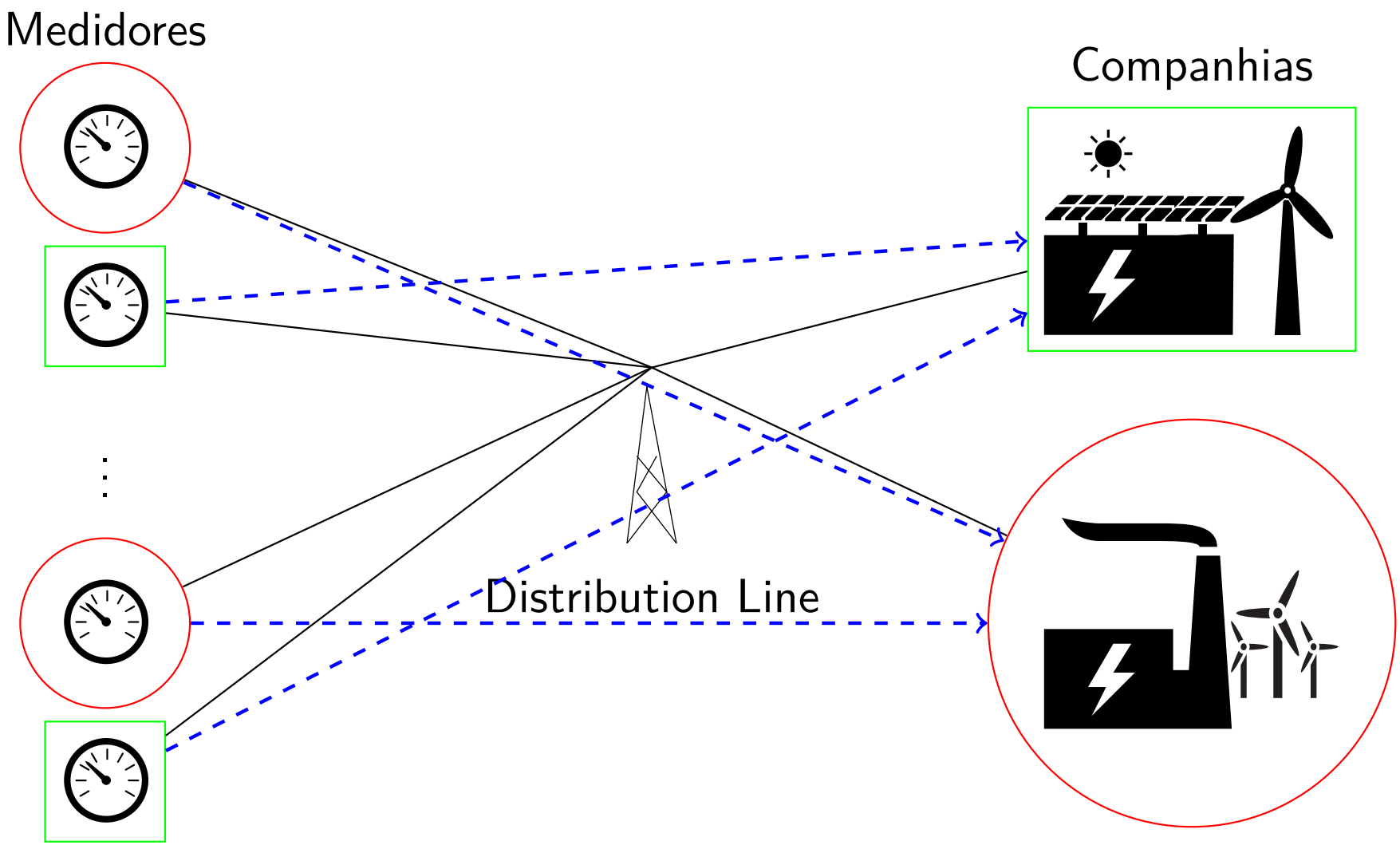
Smart Grids

[Oli17g; Bor16]



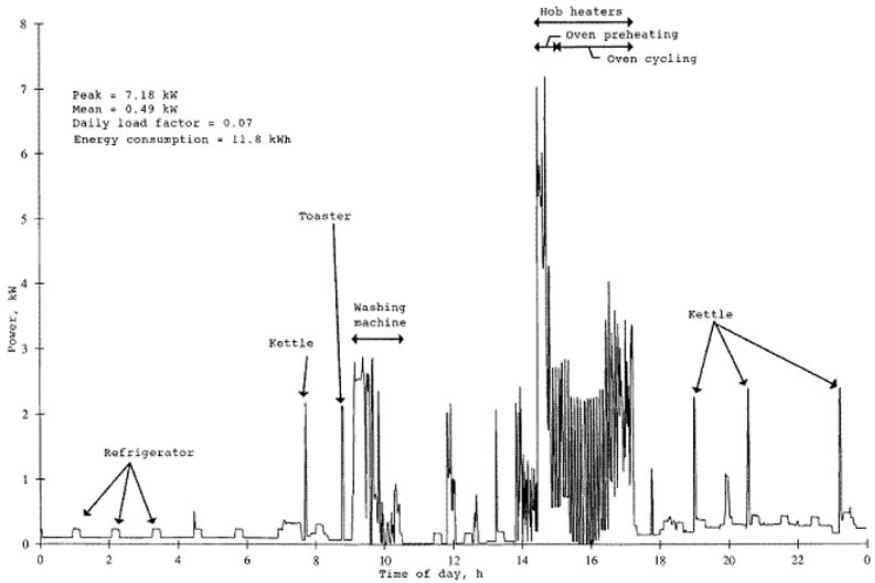
Smart Grids

[Oli17g; Bor16]

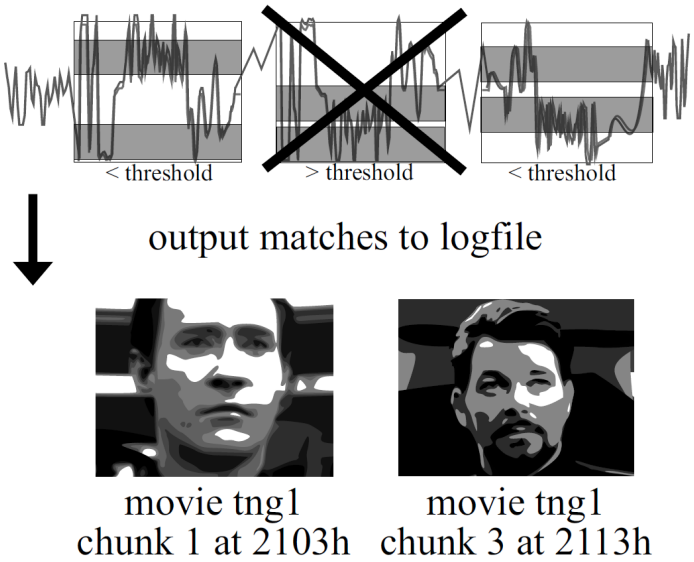


O Problema da Privacidade

[Oli17e]



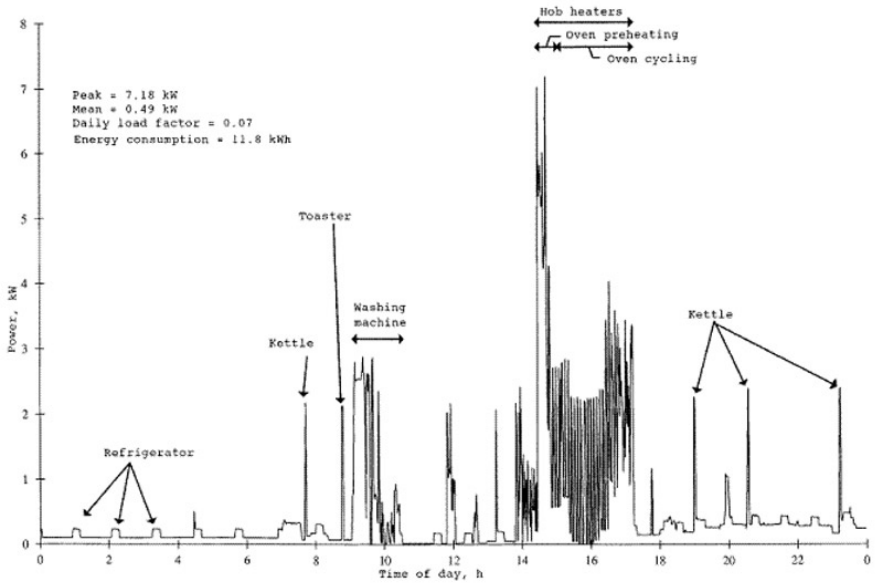
[NIST]



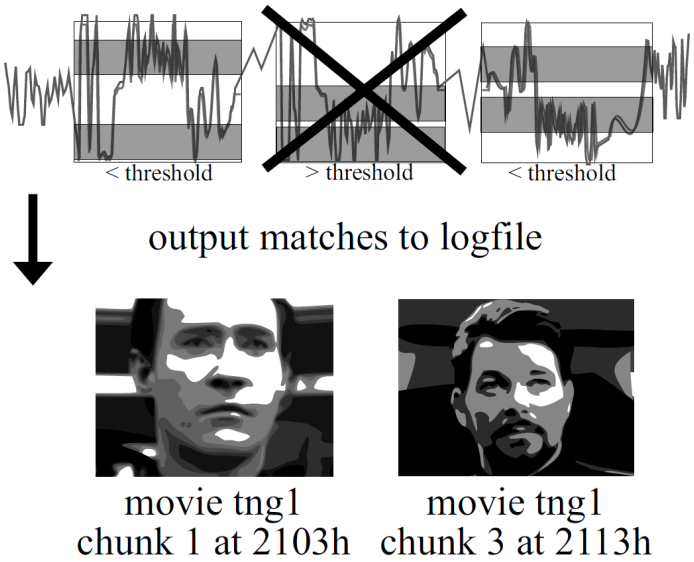
[GrevelerJL2012]

O Problema da Privacidade

[Oli17e]



[NIST]

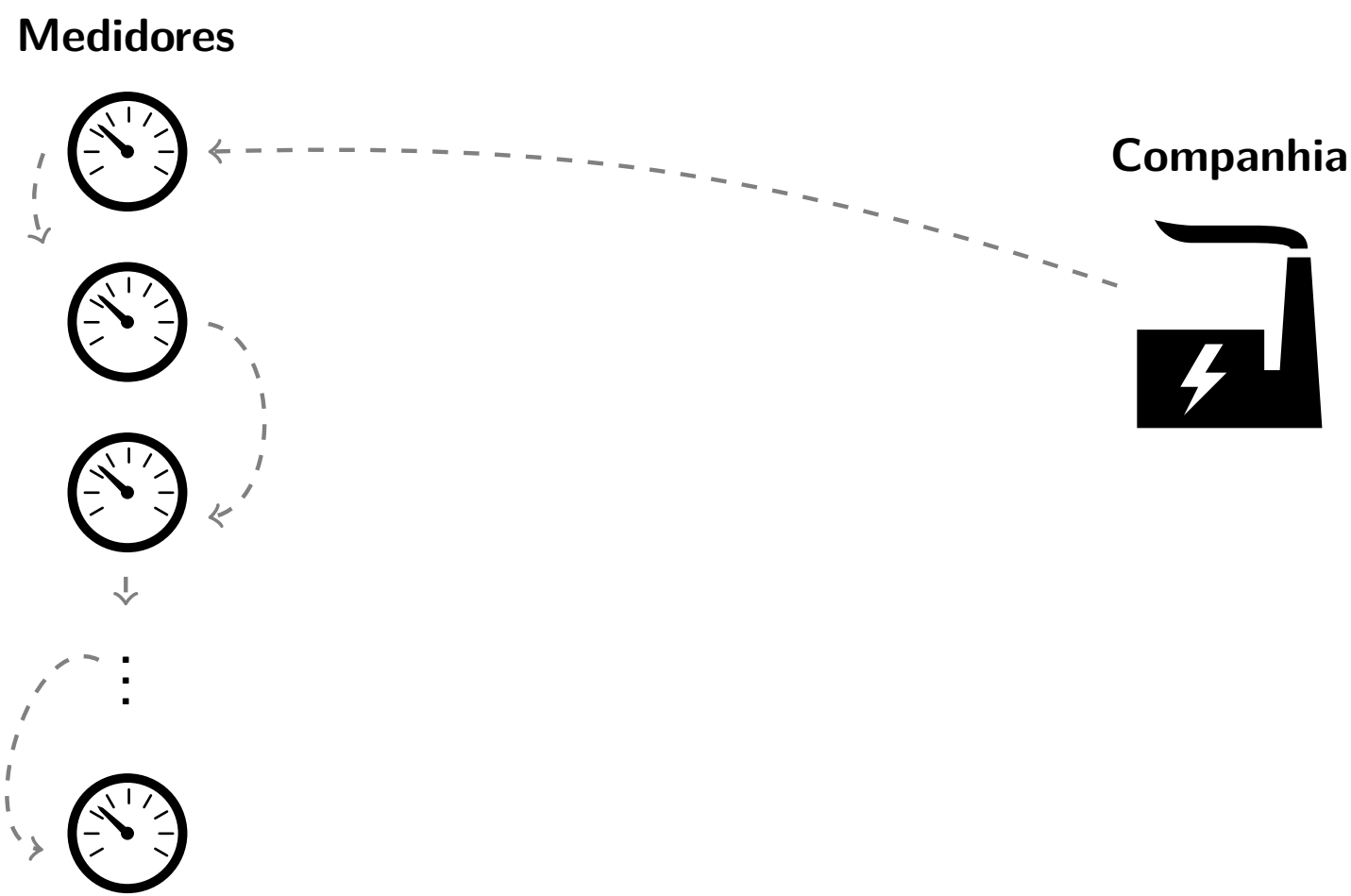


[GreverJL2012]

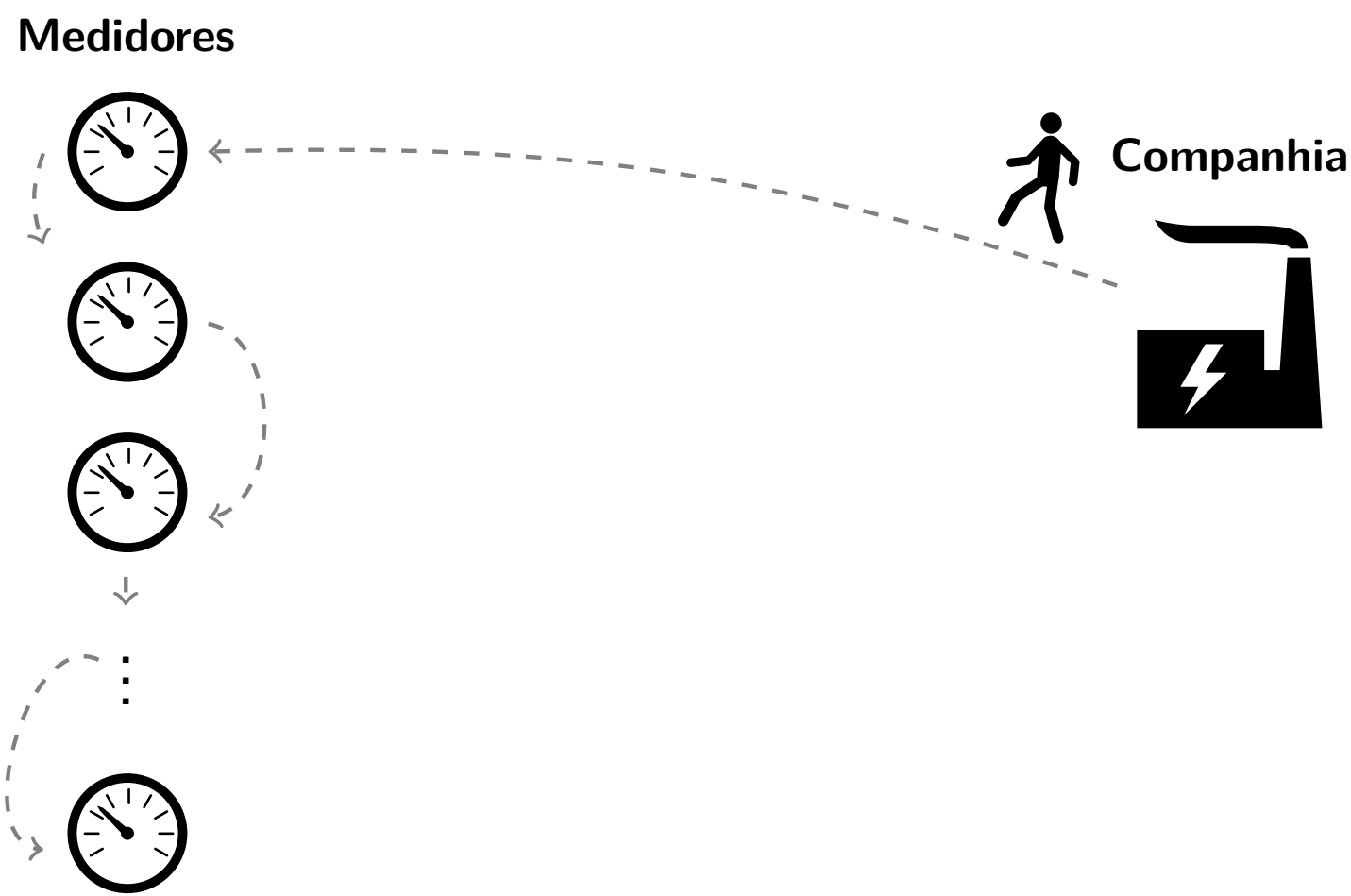
EU - Official Journal L No.315

80% dos lares equipados com smart meters em 2020 na UE

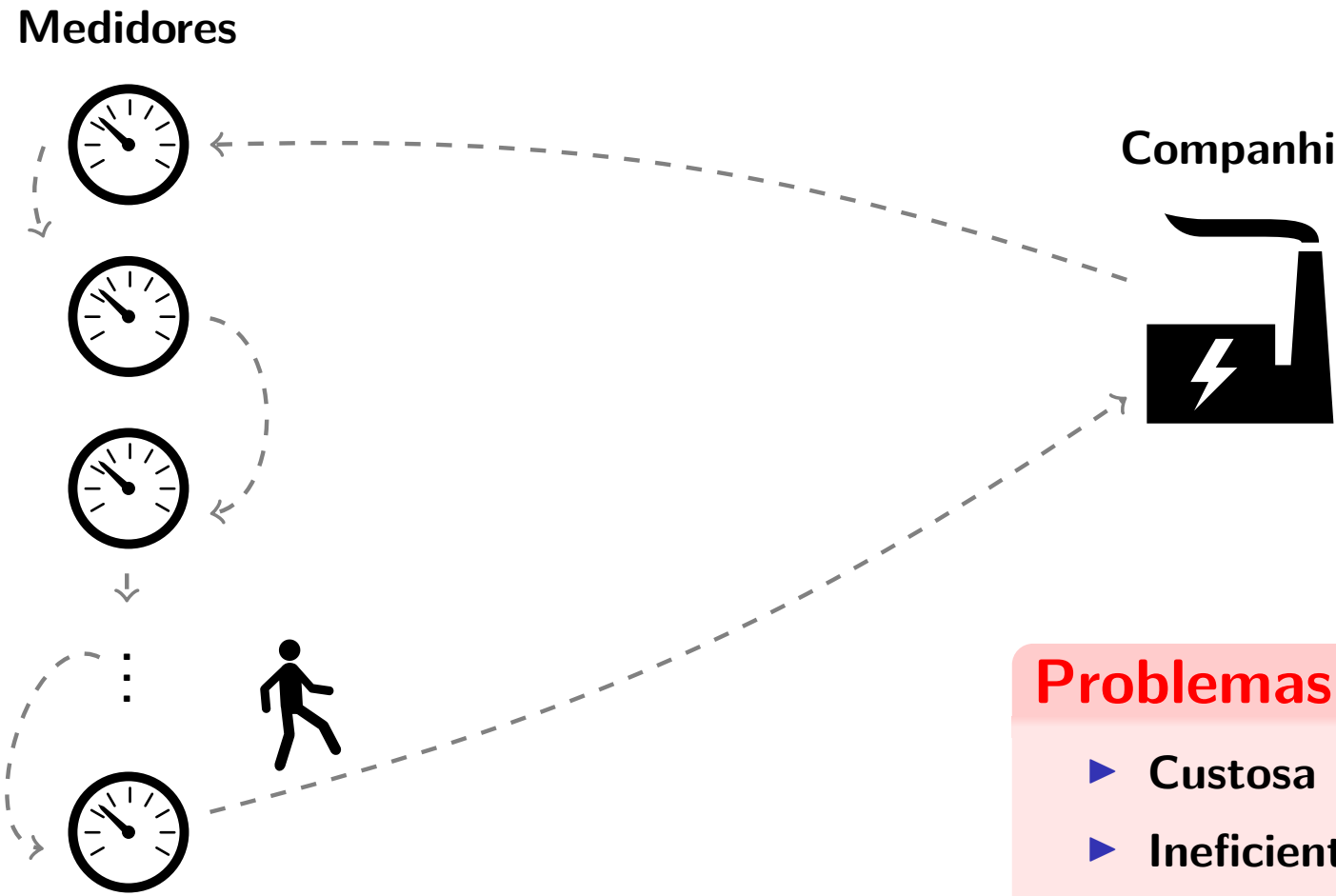
Non-smart Grid



Non-smart Grid



Non-smart Grid

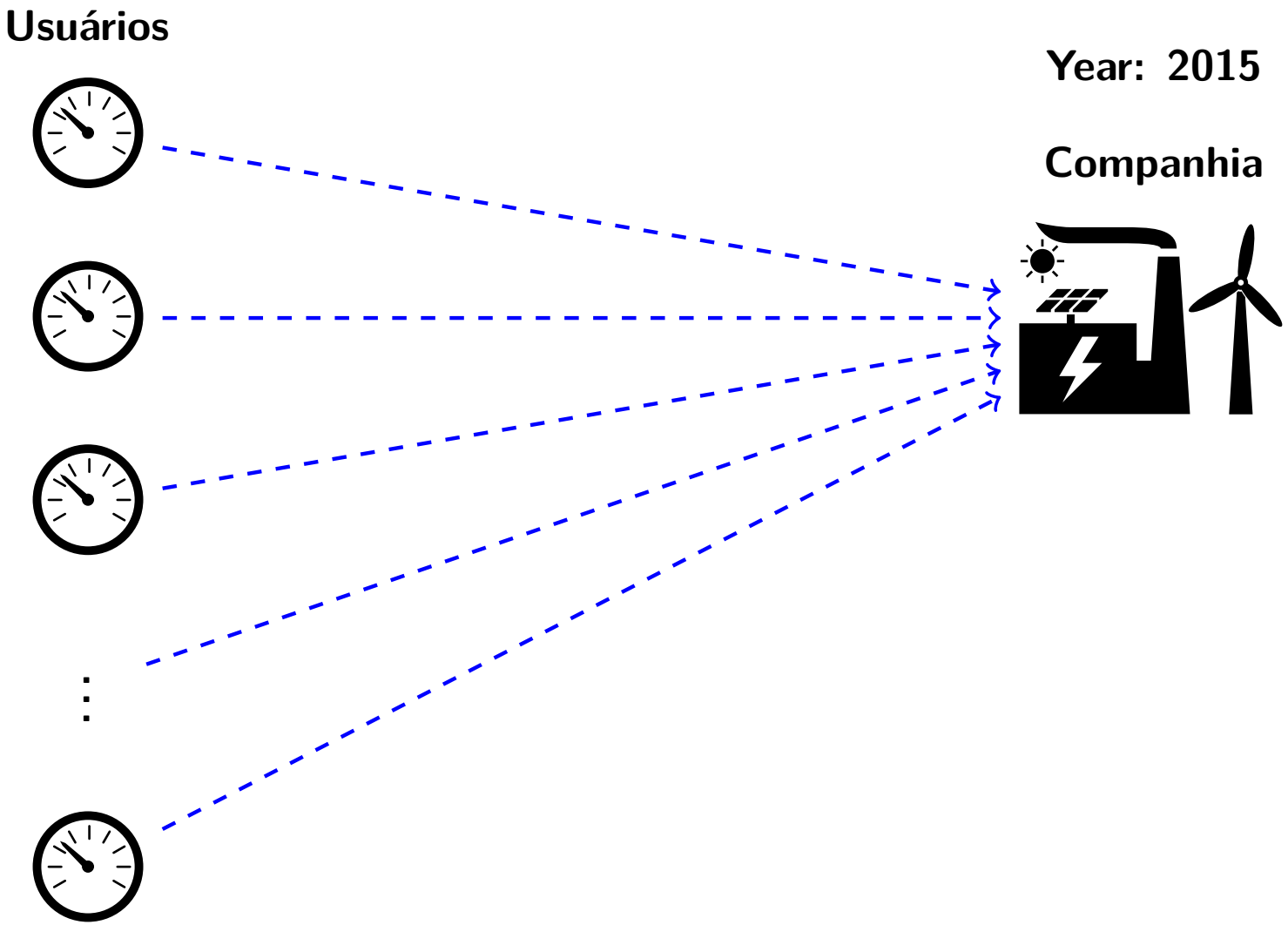


Problemas

- Custosa
- Ineficiente
- Fraudes

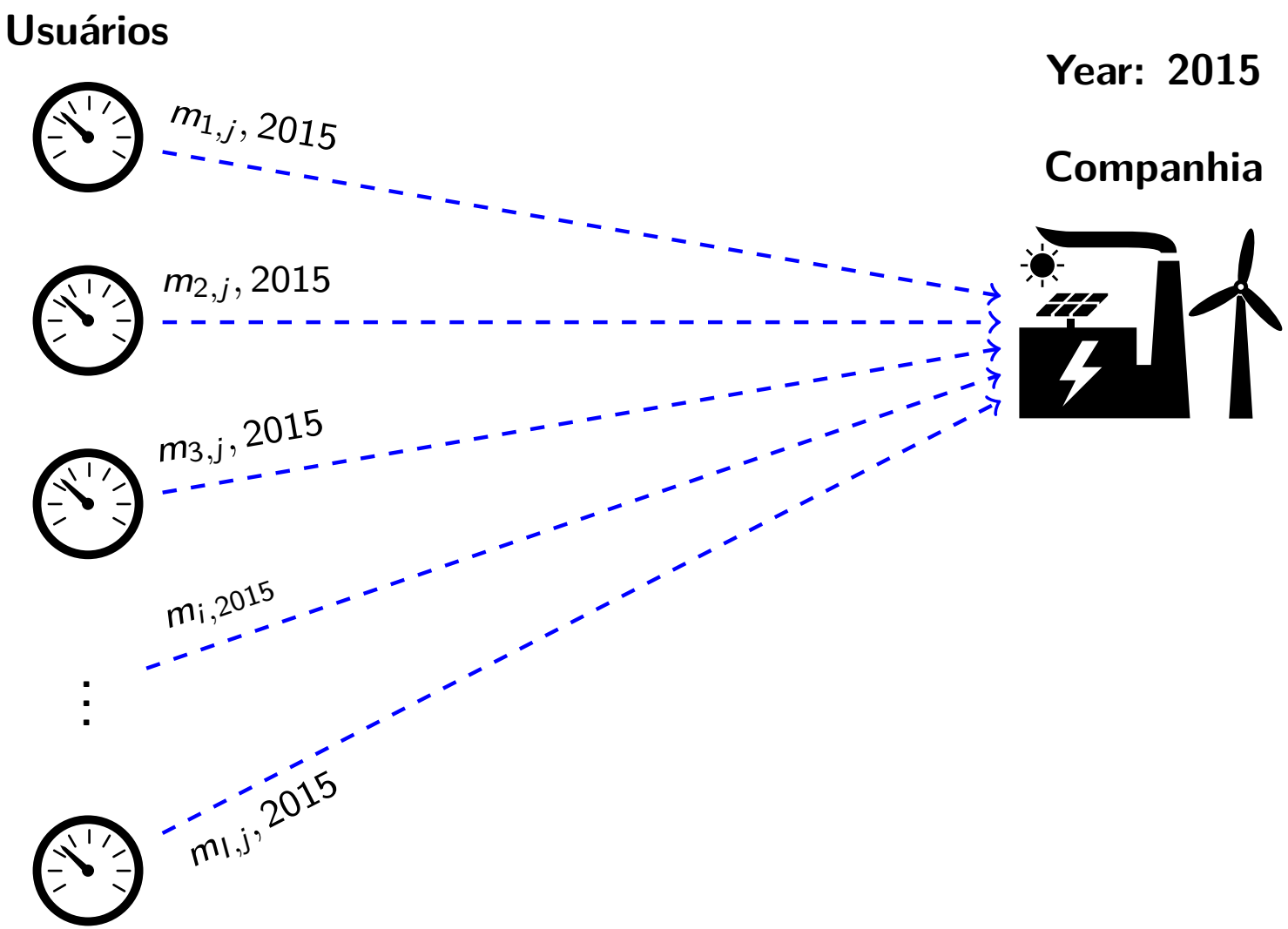
Tornando Inteligente

Coletando medições anualmente



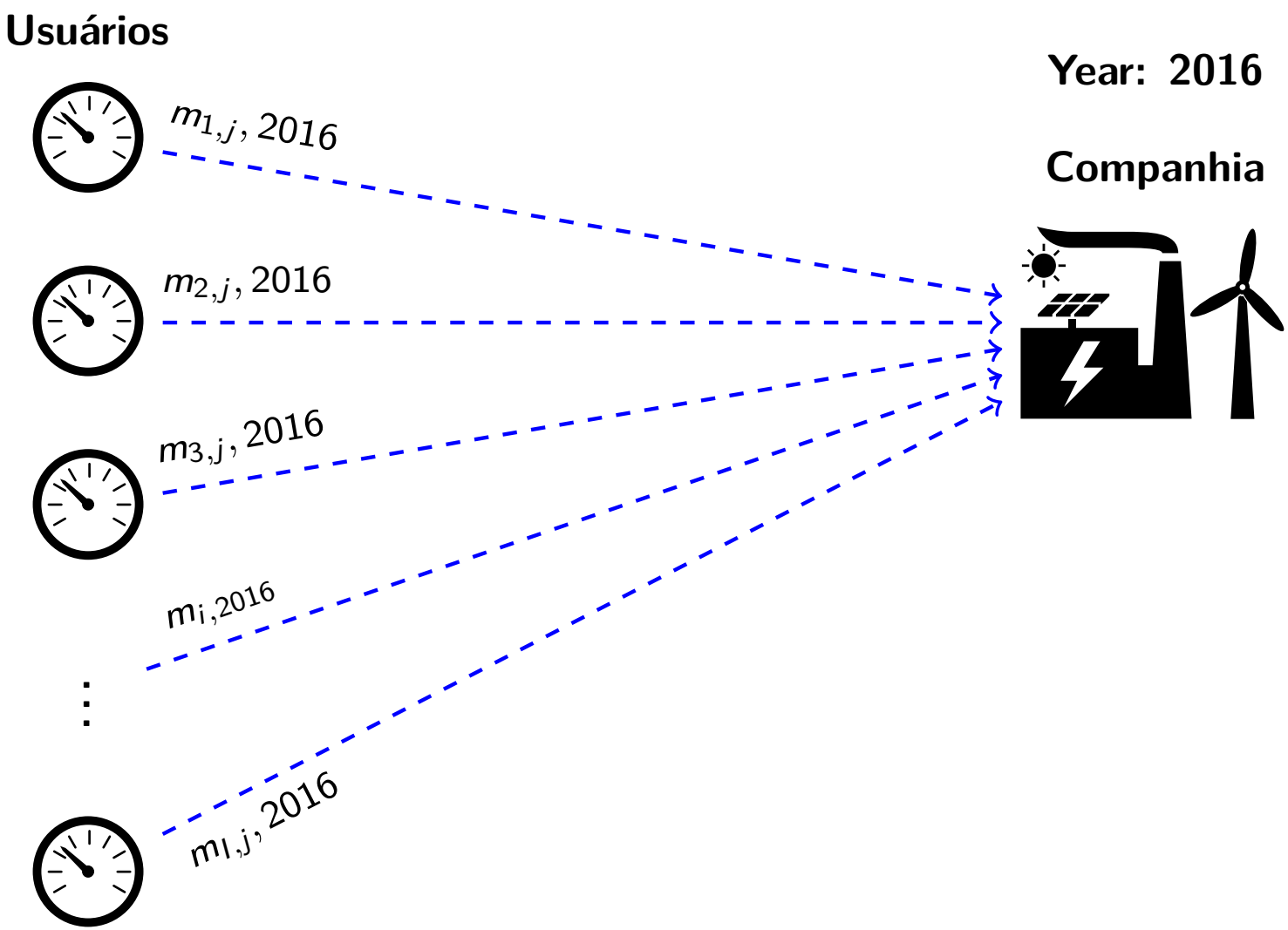
Tornando Inteligente

Coletando medições anualmente



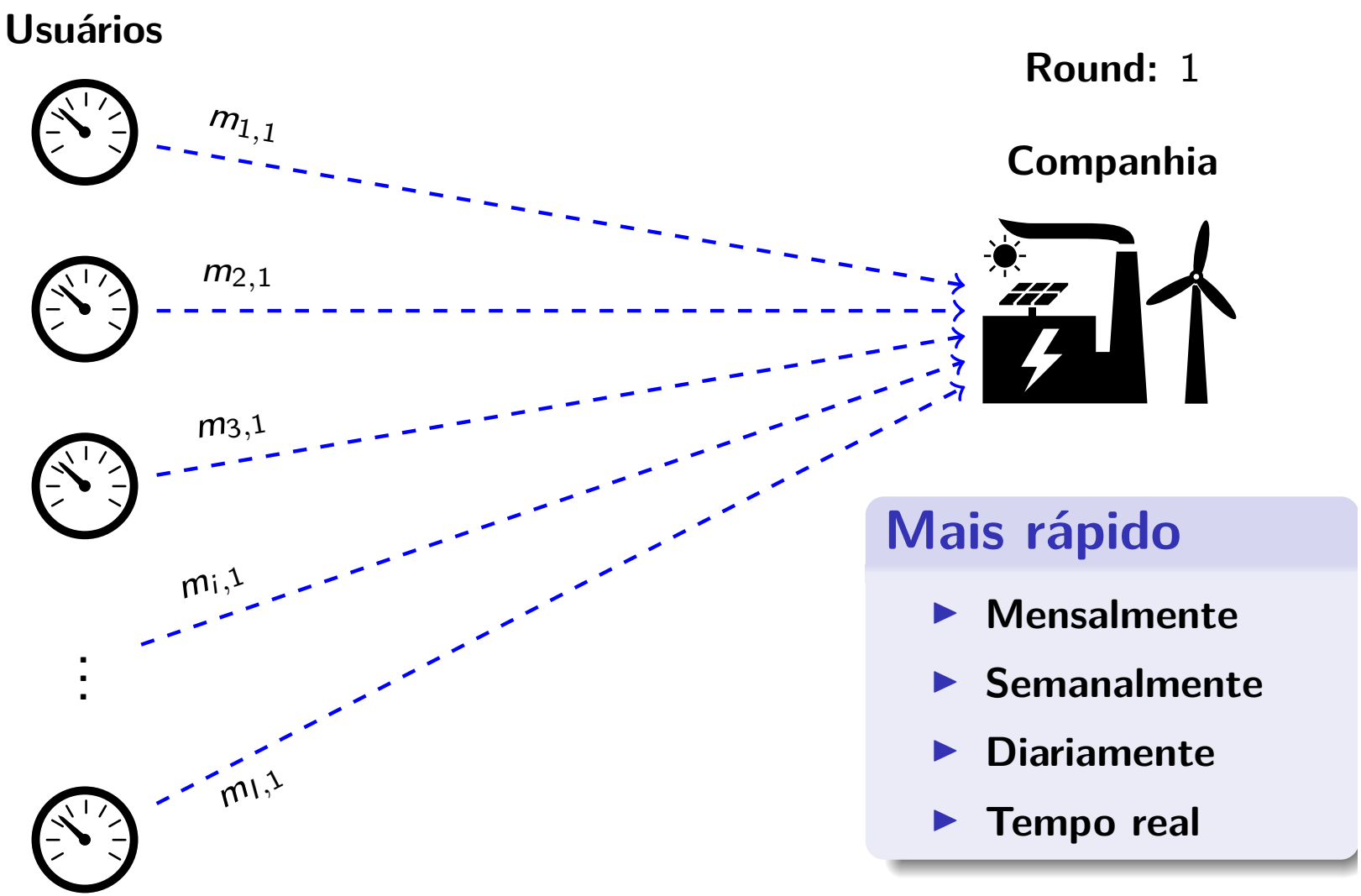
Tornando Inteligente

Coletando medições anualmente



Tornando Inteligente

Coletando medições anualmente

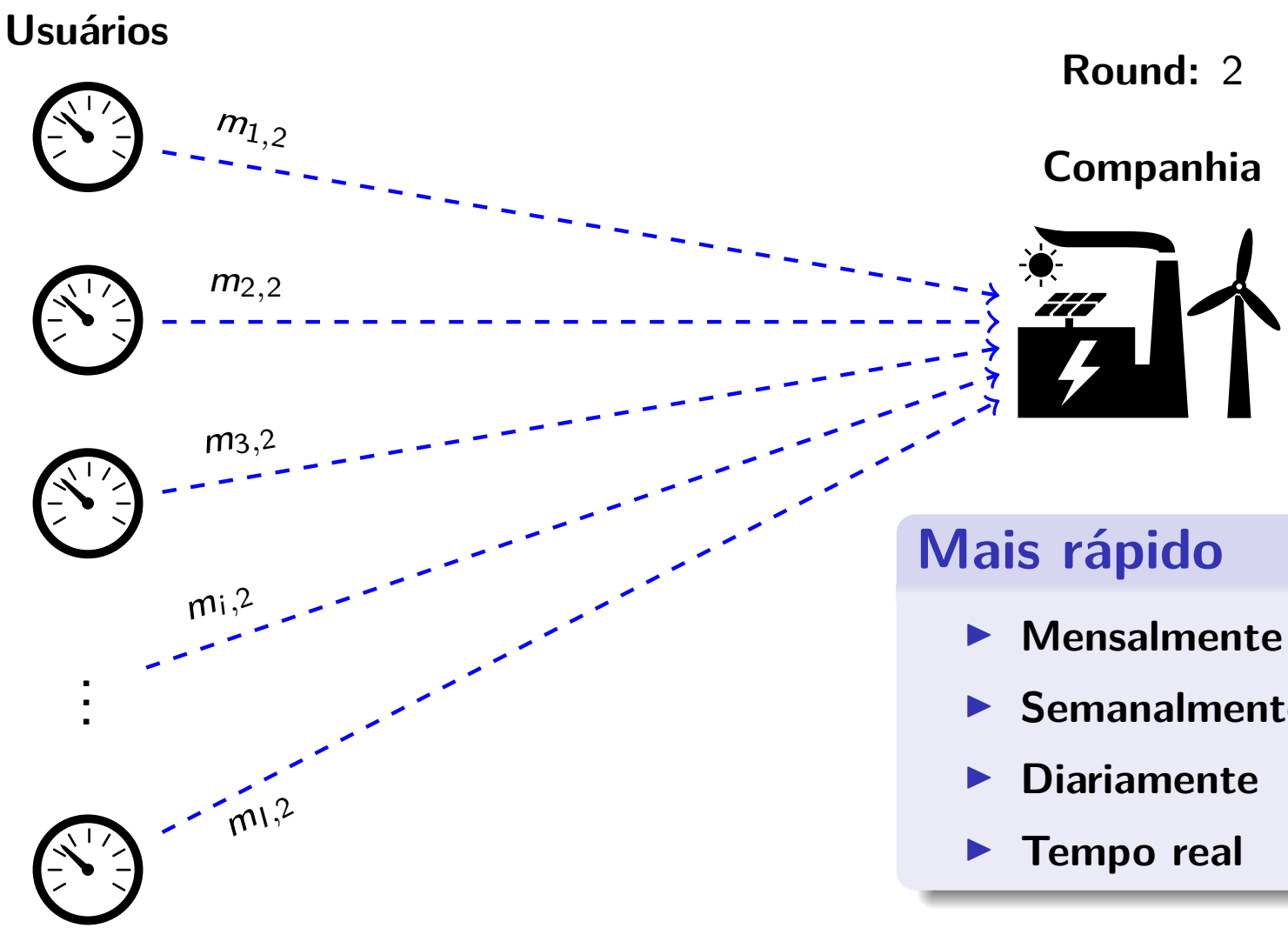


Mais rápido

- Mensalmente
- Semanalmente
- Diariamente
- Tempo real

Tornando Inteligente

Coletando medições anualmente

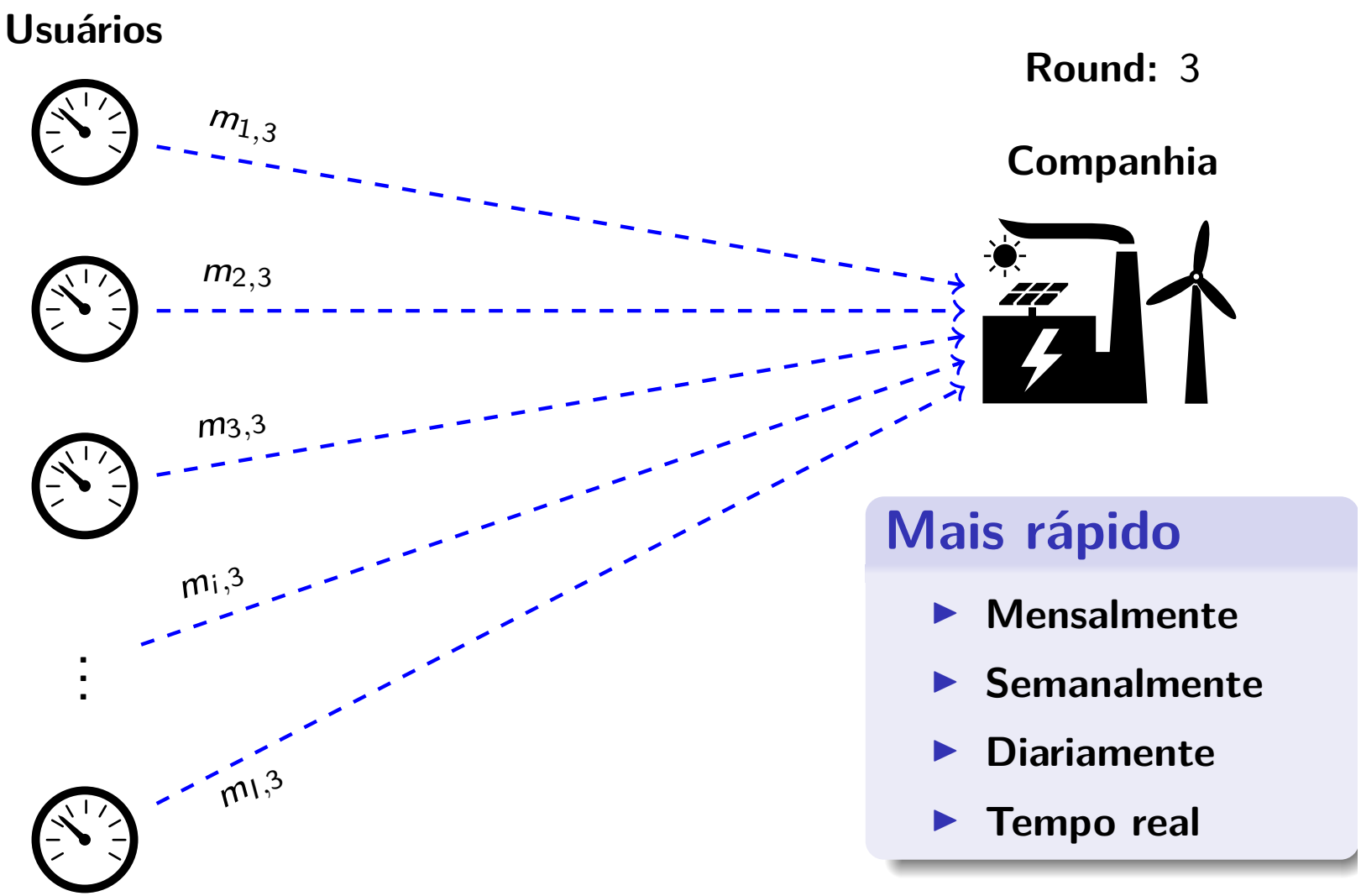


Mais rápido

- Mensalmente
- Semanalmente
- Diariamente
- Tempo real

Tornando Inteligente

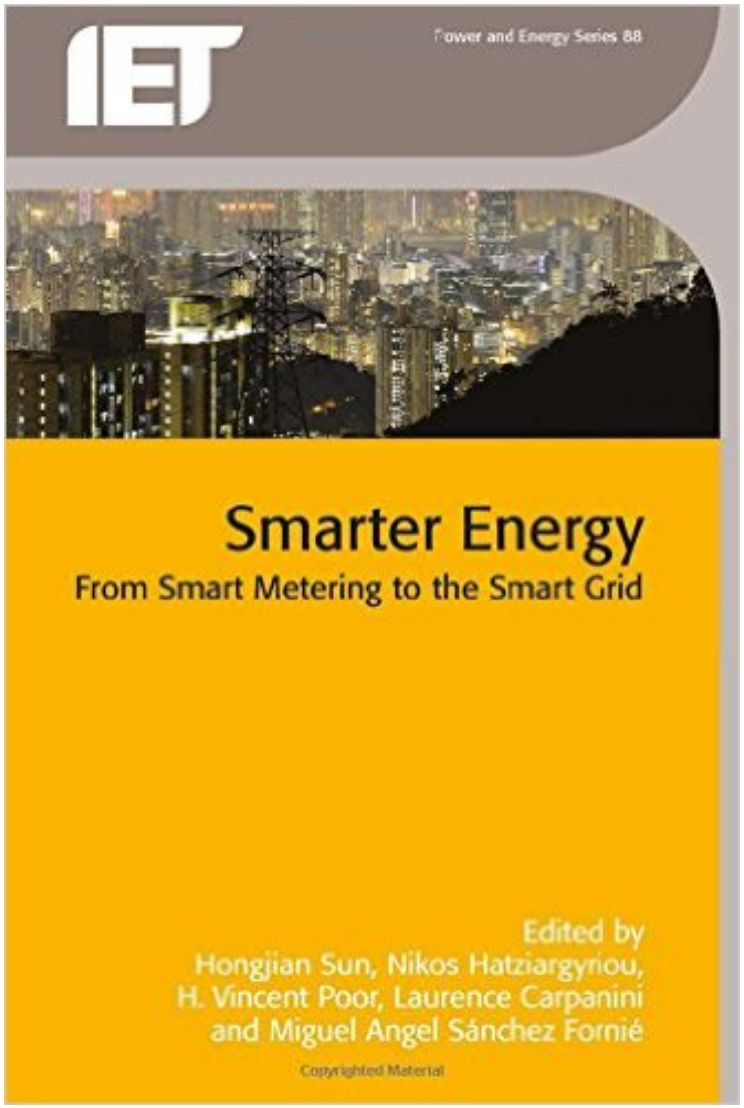
Coletando medições anualmente

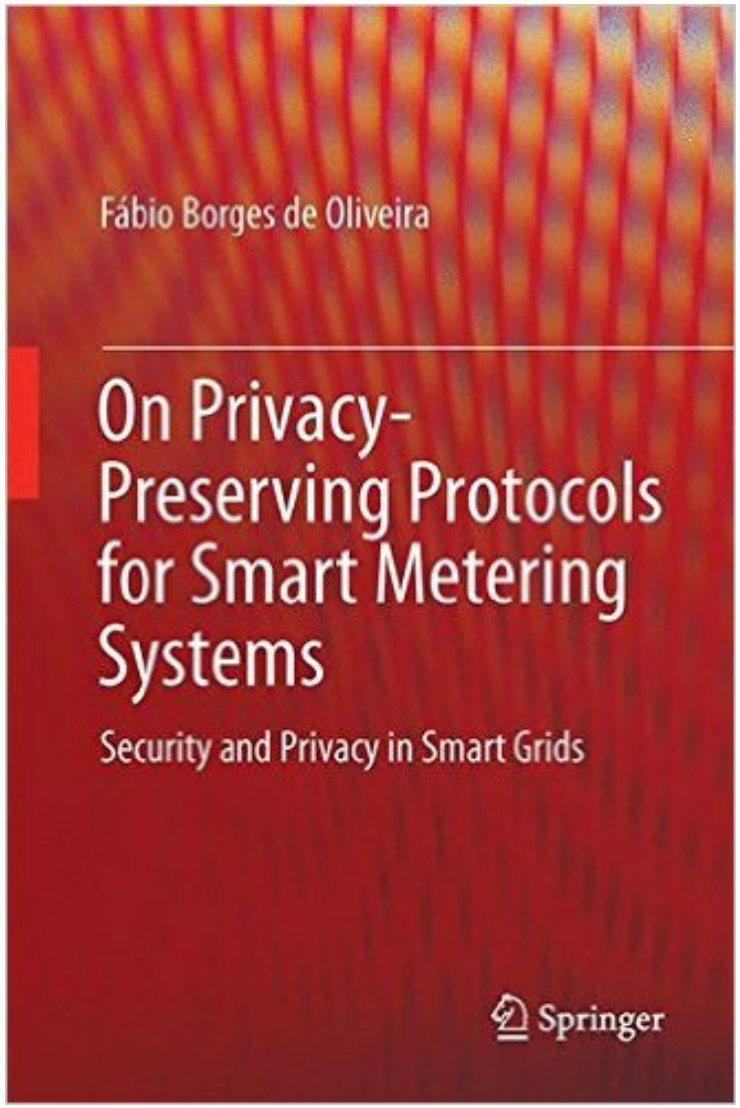


Mais rápido

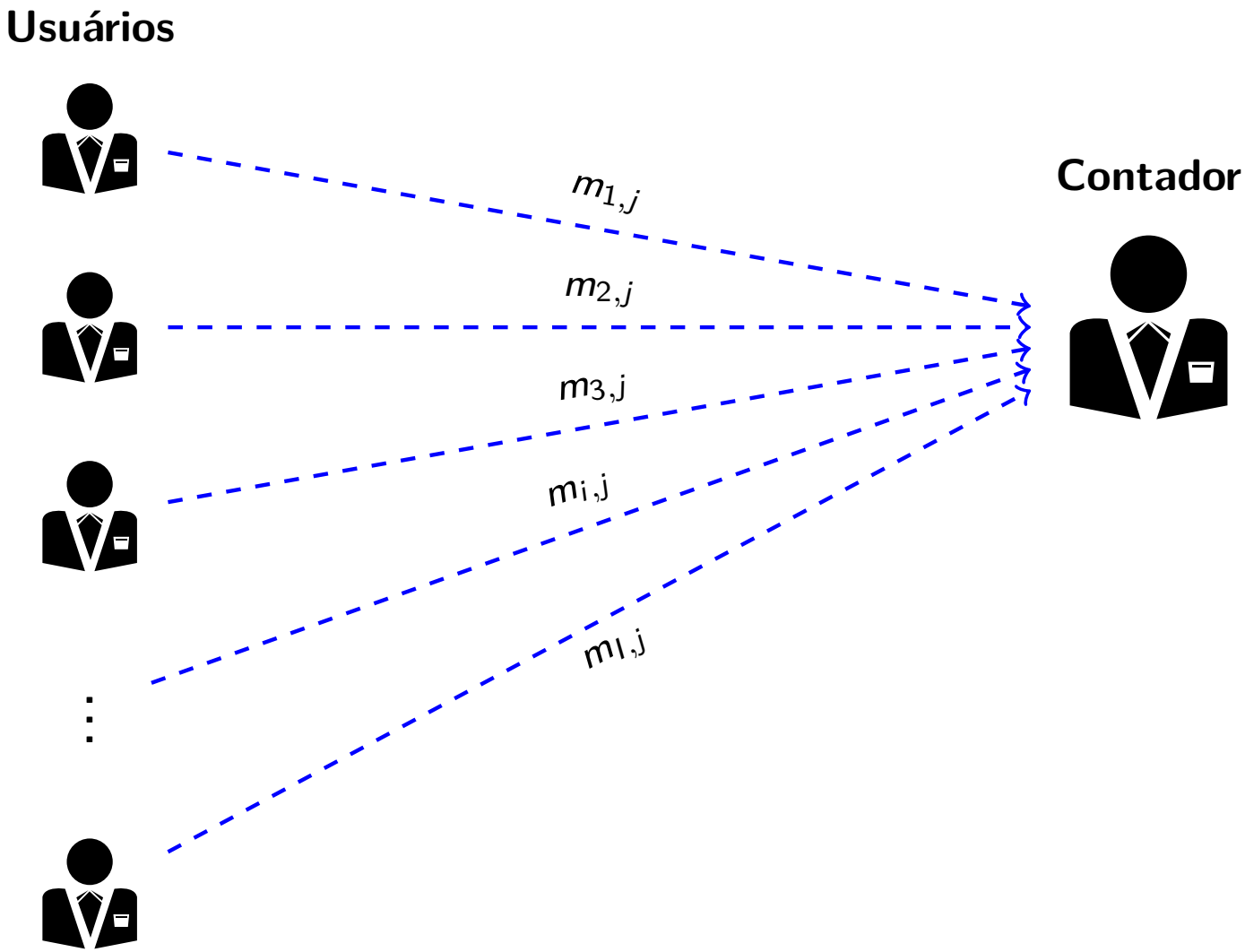
- Mensalmente
- Semanalmente
- Diariamente
- Tempo real

Referências

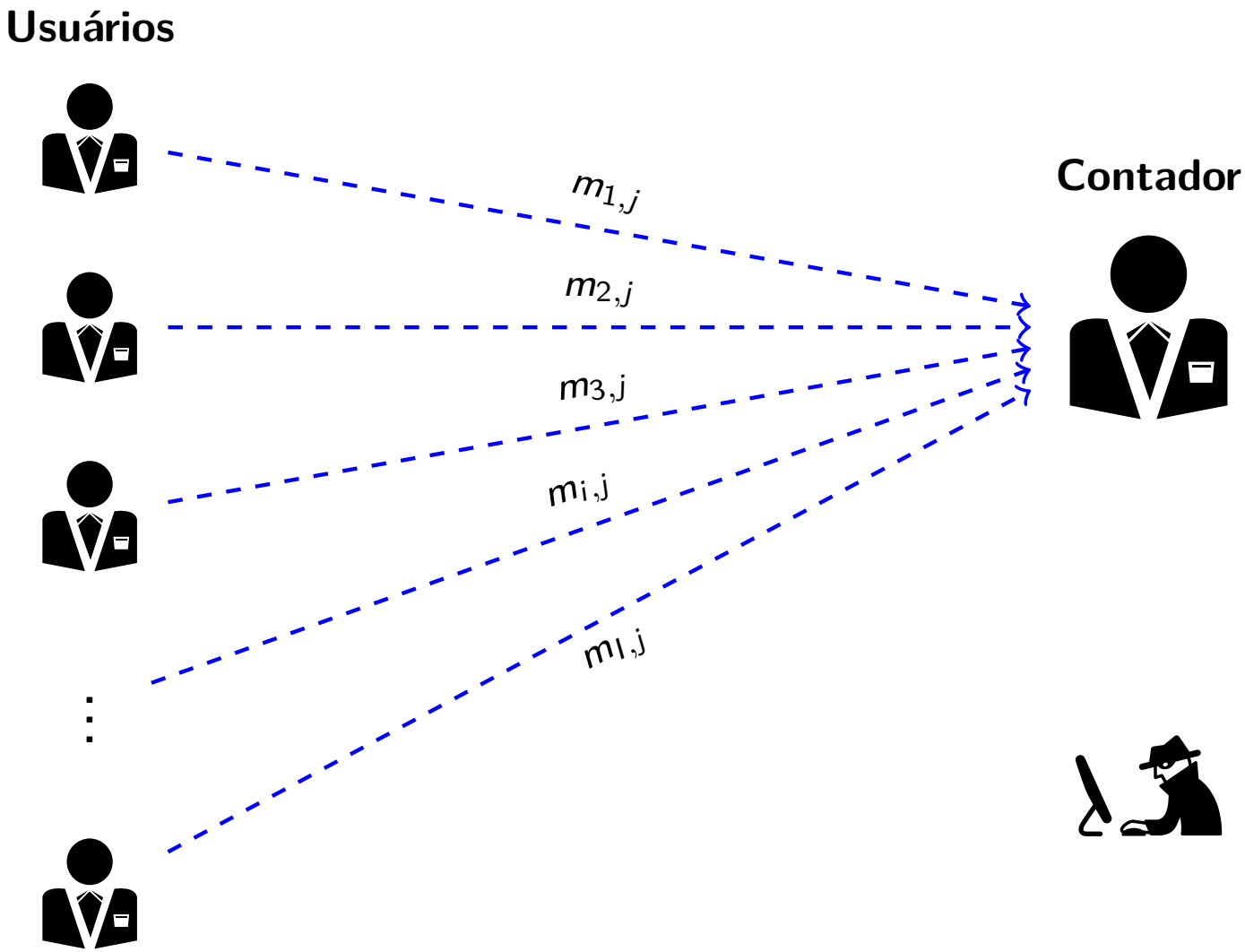




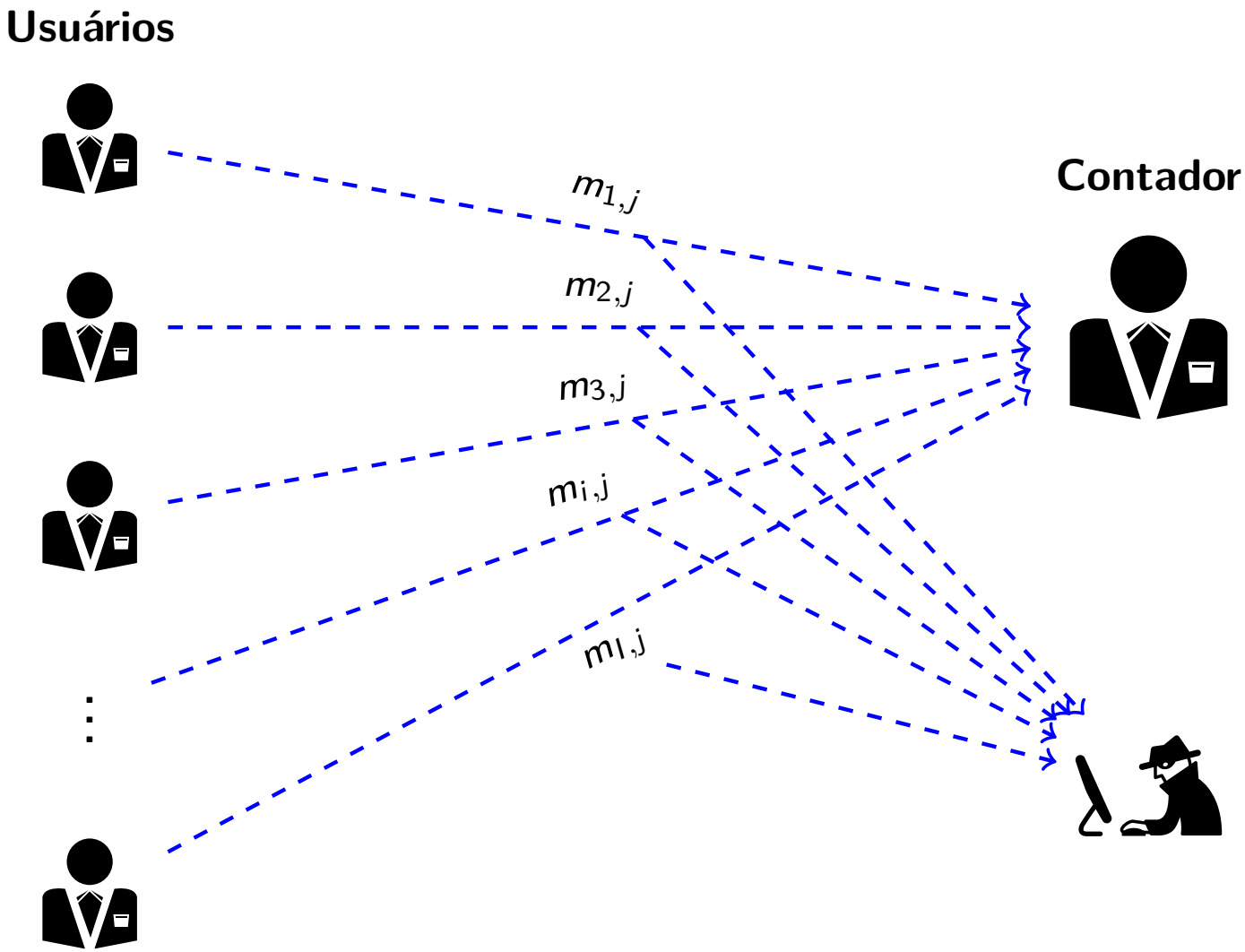
Necessidade de Criptografia



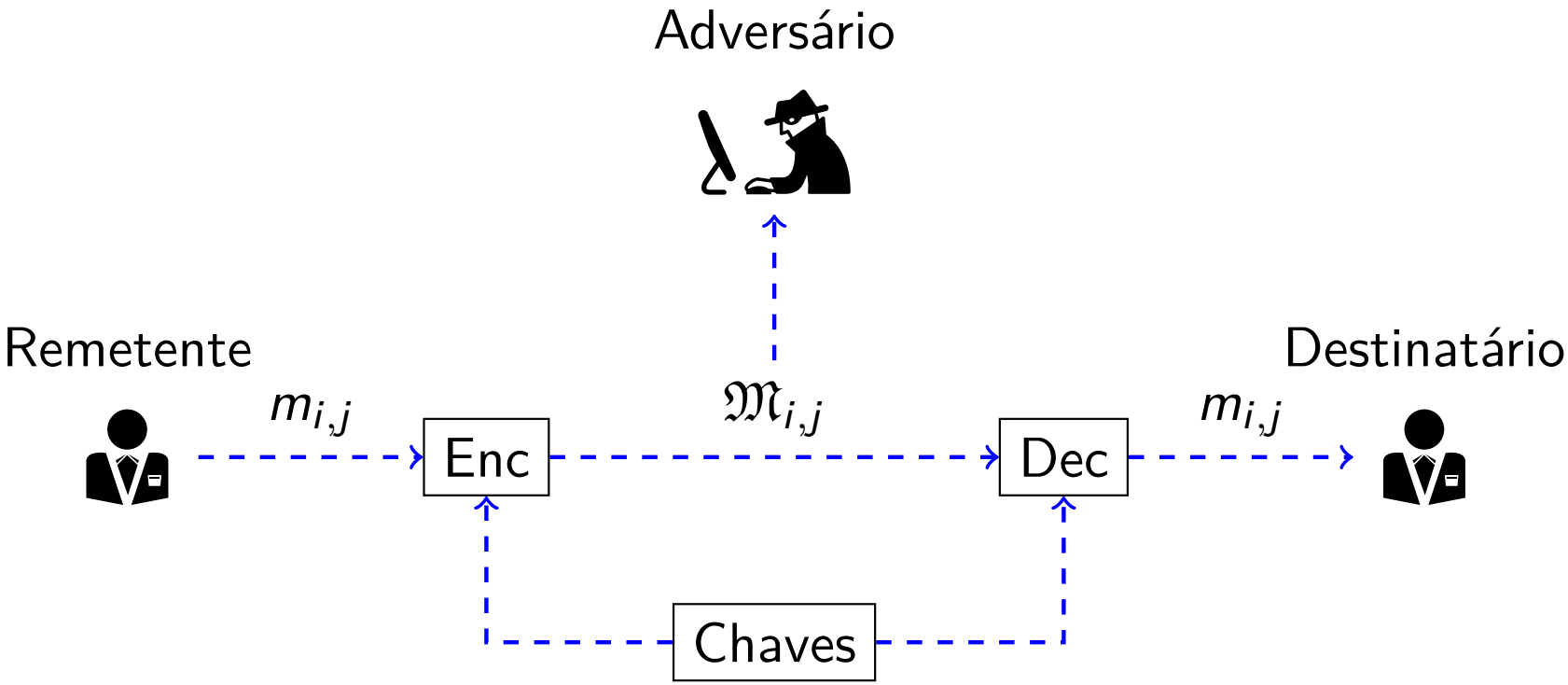
Necessidade de Criptografia



Necessidade de Criptografia

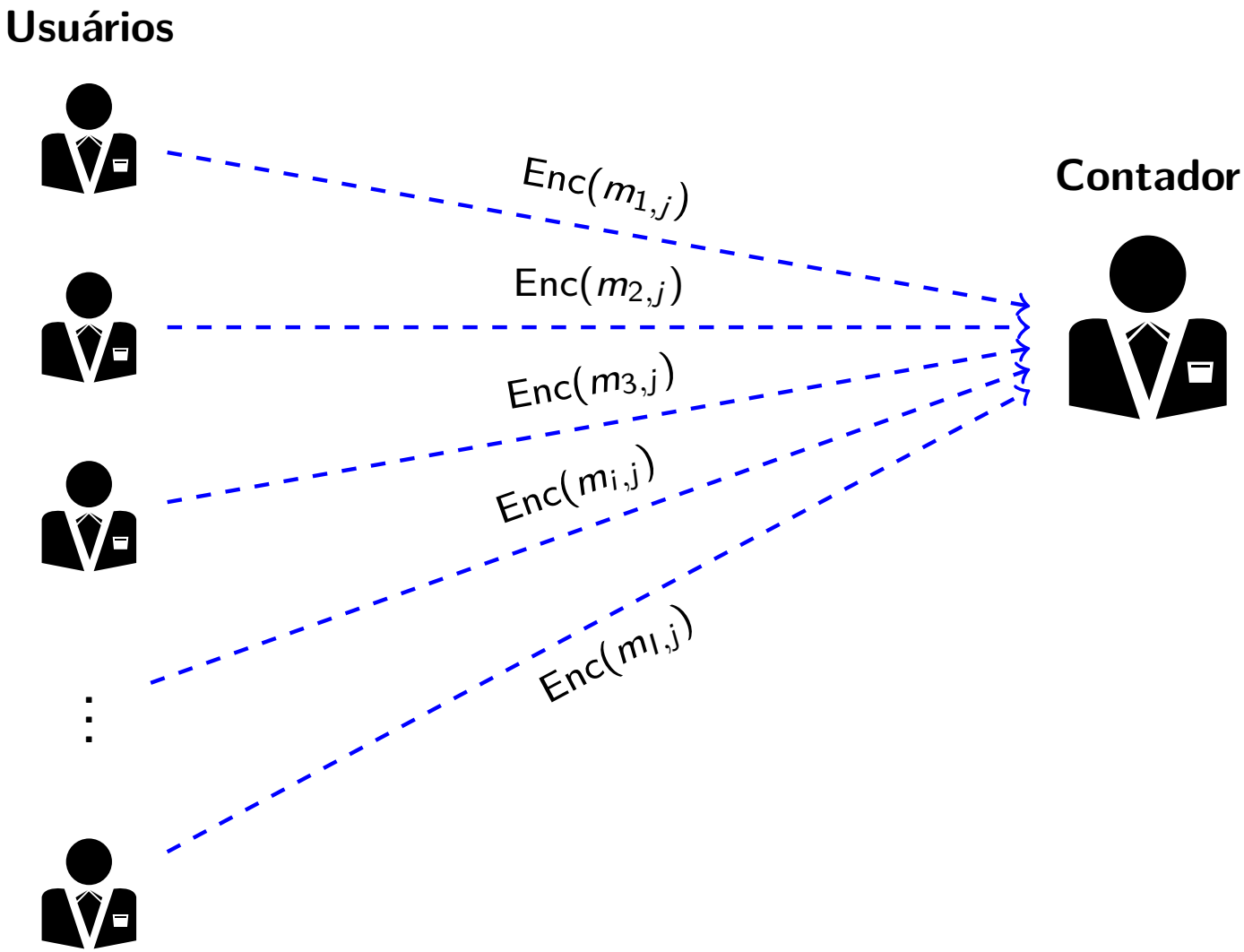


Shannon


Adversário
Remetente
$m_{i,j}$
Enc
$\mathfrak{M}_{i,j}$
Dec
$m_{i,j}$
Destinatário
Chaves

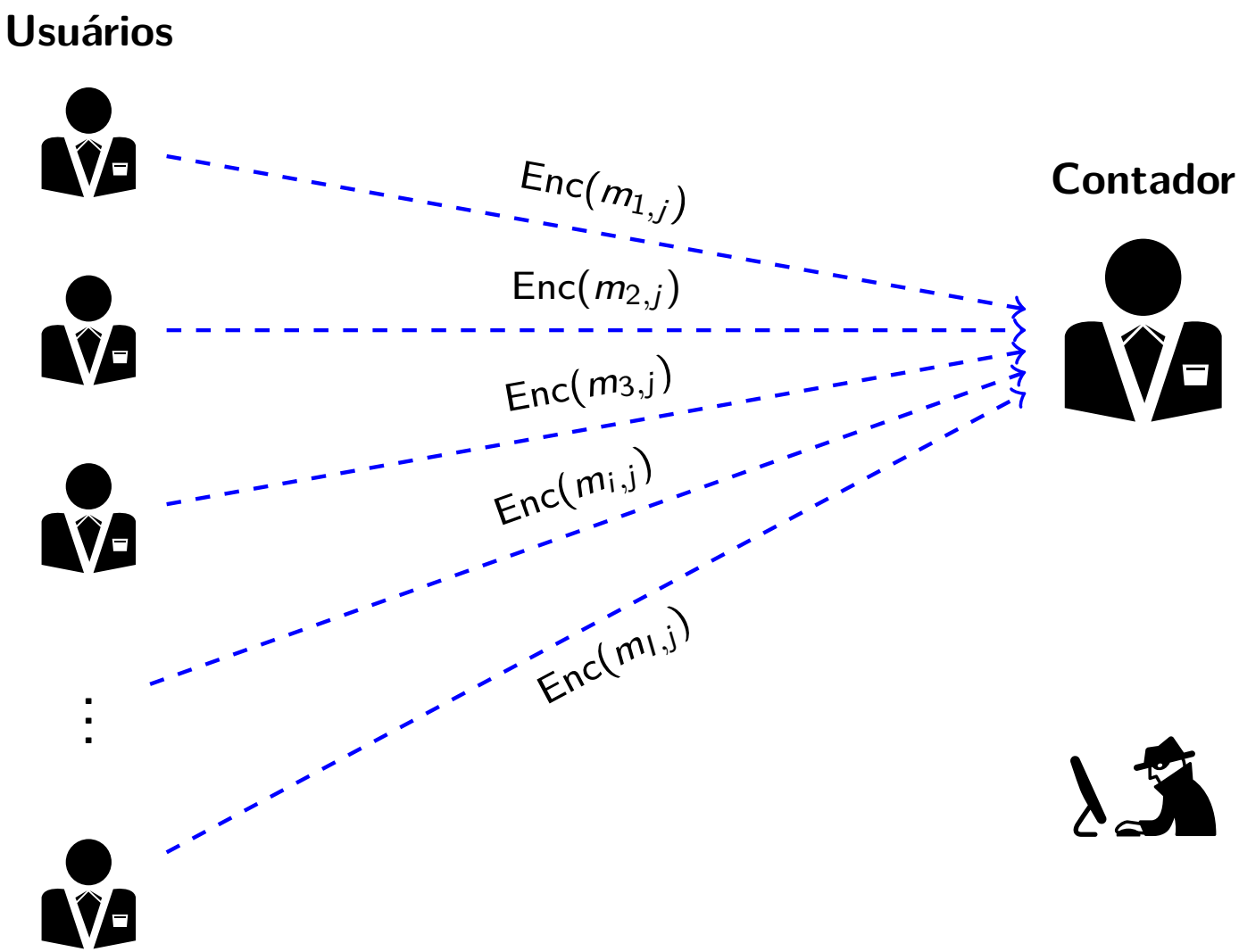
Necessidade de Consolidação

Agregação



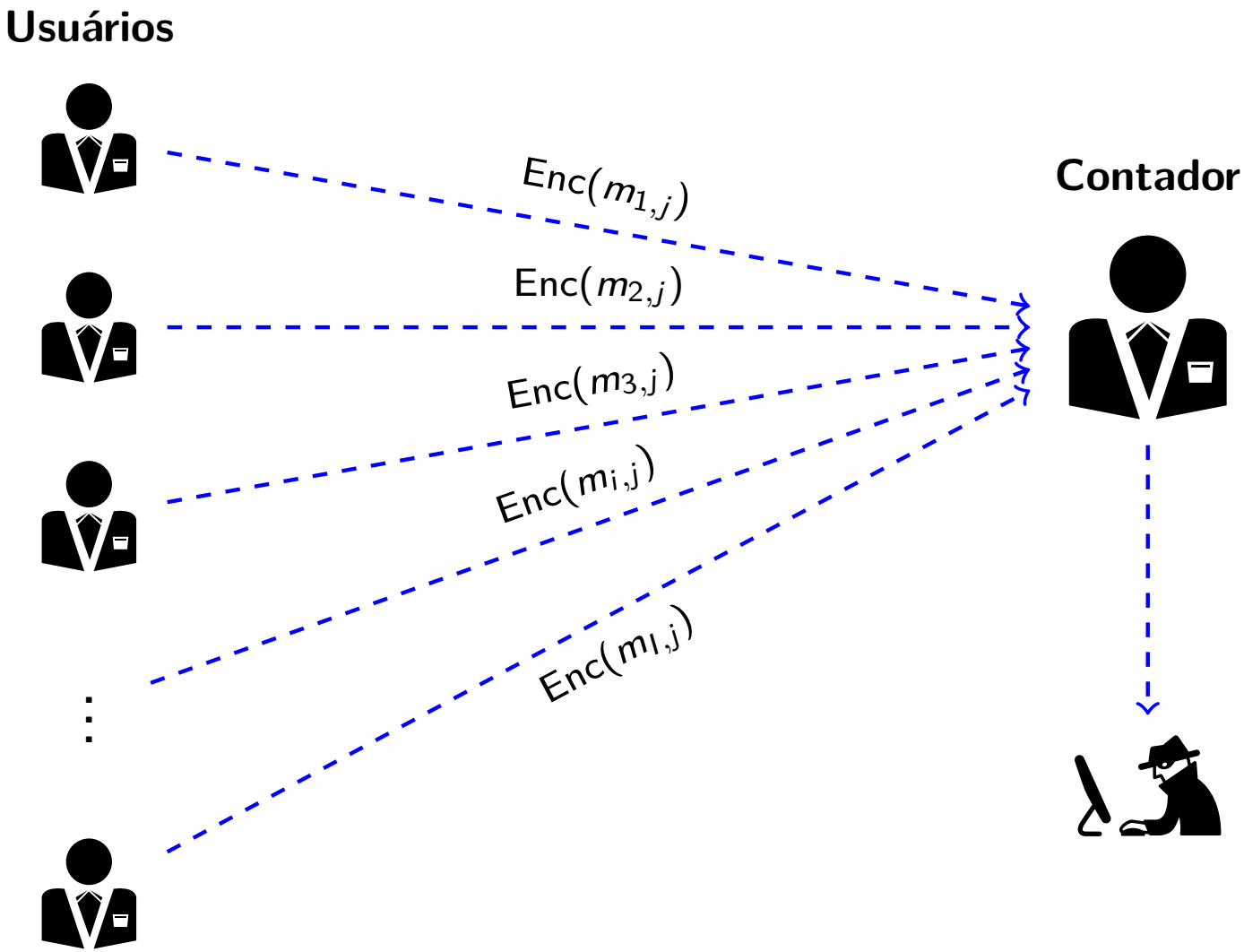
Necessidade de Consolidação

Agregação



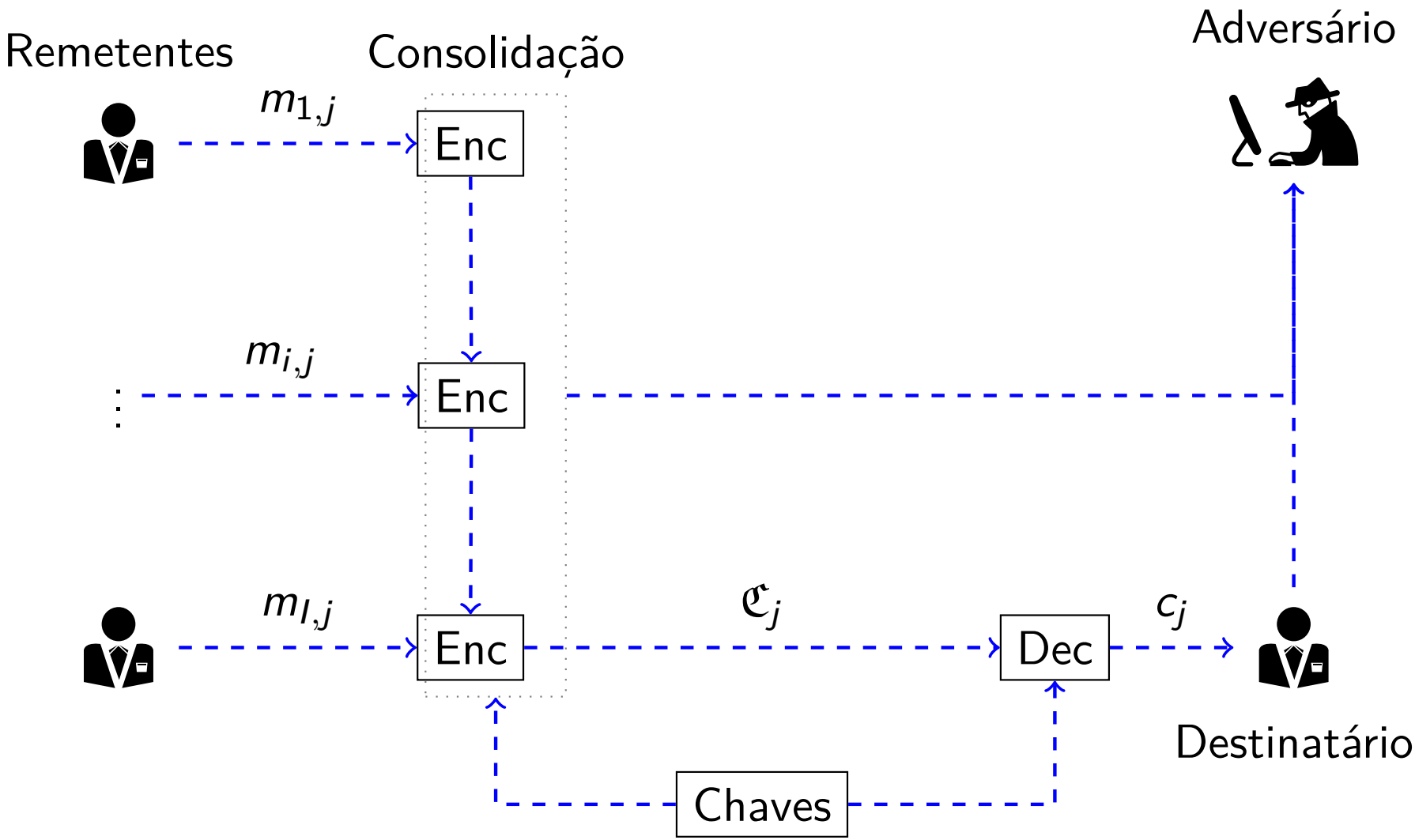
Necessidade de Consolidação

Agregação



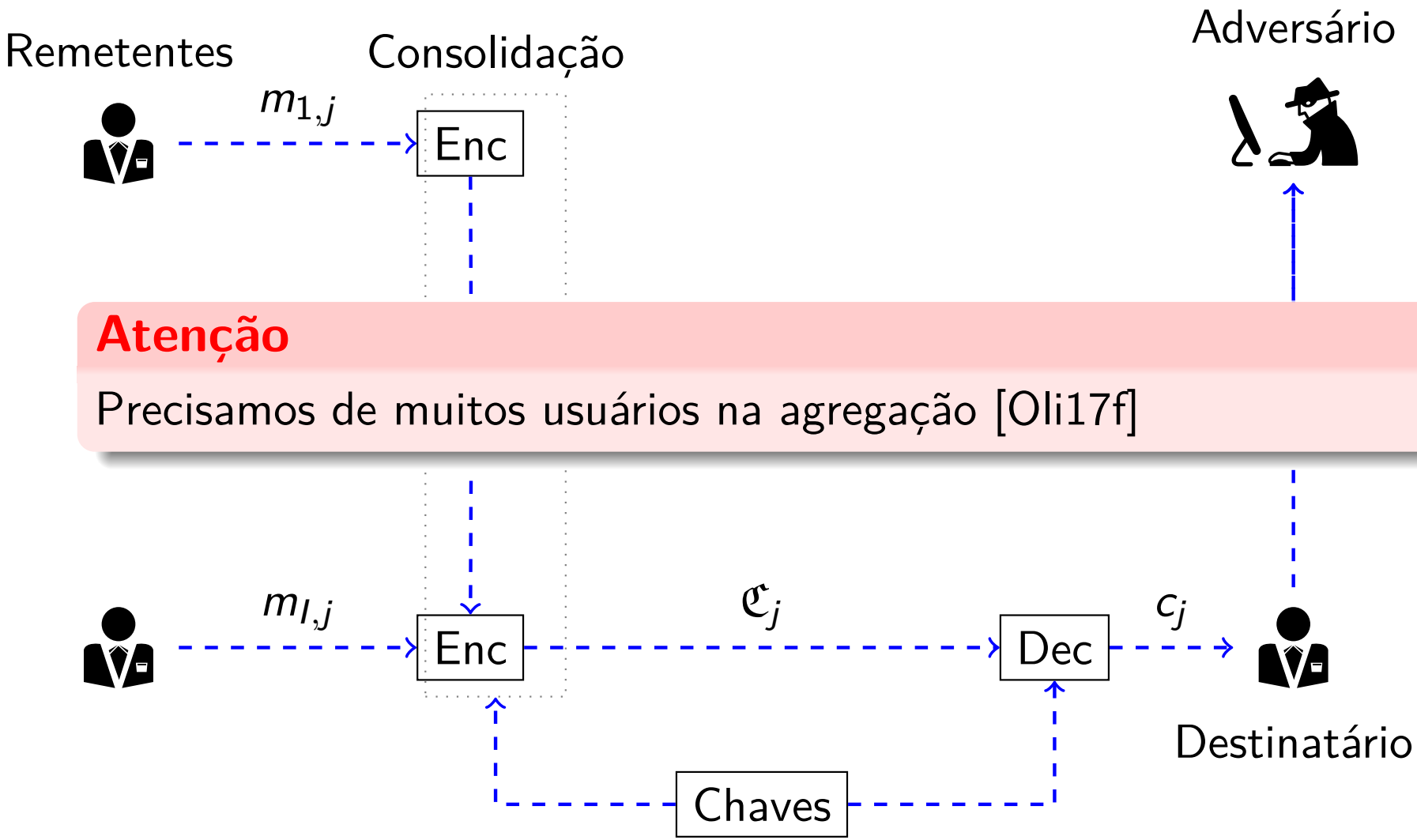
Consolidação

Agregação [Oli17c]



Consolidação

Agregação [Oli17c]

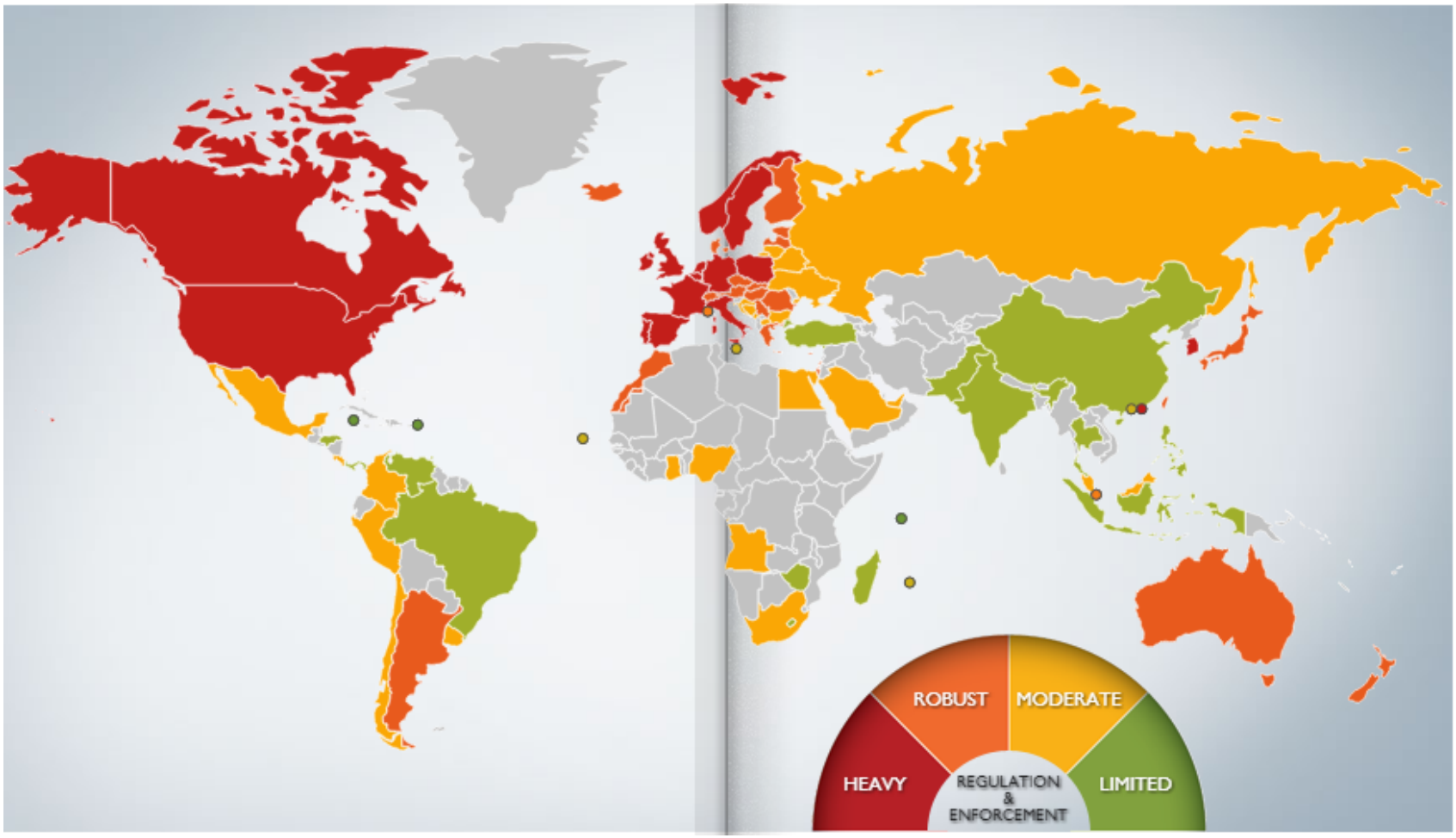


Atenção

Precisamos de muitos usuários na agregação [Oli17f]

Segurança versus Privacidade

Leis de Proteção



[https://www.dlapiperdataprotection.com/#handbook/world-map-section]

Tópicos

Definição de Métrica

Dado um conjunto $\mathcal{C}$ e uma função $d : \mathcal{C} \times \mathcal{C} \to \mathbb{R}^+$, onde $\mathbb{R}^+$ representa o conjunto dos números reais não-negativos, dizemos que d é uma métrica se as seguintes condições são satisfeitas para todo $x, y, z \in \mathcal{C}$:

1. $d(x, y) \geqslant 0$ positivamente definida
2. $d(x, y) = 0 \Leftrightarrow x = y$ identidade
3. $d(x, y) = d(y, x)$ simetria
4. $d(x, z) \leq d(x, y) + d(y, z)$ desigualdade triangular

Privacidade Diferencial

O algoritmo probabilístico $\mathcal{A}$ é privado ϵ-diferencialmente se para toda base de dados D_1 e D_2 que difere em um único elemento, e para todos os subconjuntos de S da imagem de $\mathcal{A}$, temos

$$\Pr[\mathcal{A}(D_1) \in S] \leq e^{\epsilon} \times \Pr[\mathcal{A}(D_2) \in S].$$

Entropia

Grau de anonimato g

$$H(X) = \sum_{i=1}^{N} \left[p_i \cdot \log_2 \left(\frac{1}{p_i} \right) \right],$$

onde $H(X)$ é a entropia da rede, N é o número de nós e p_i é a probabilidade associada a cada nó i. A entropia máxima ocorre quando temos uma probabilidade uniforme, i.e., todos os nós sãs equiprováveis $1/N$, o que gera

$$H_M = \log_2(N).$$

Logo, o grau de anonimato g é definido por

$$g = 1 - \frac{H_M - H(X)}{H_M} = \frac{H(X)}{H_M}.$$

Complexidade

[Oli17f]

Insuficiente:

1. complexidade do algoritmo
2. grau de anonimato - entropia
3. privacidade diferencial

Complexidade

[Oli17f]

Insuficiente:

1. complexidade do algoritmo
2. grau de anonimato - entropia
3. privacidade diferencial

Solução

Complexidade do Problema

Contagem e Probabilidades

1. caso binário de consolidação
2. caso geral de consolidação

$$7 = x_1 + x_2 + x_3 \Longrightarrow \boxed{\star\star\star\star}\boxed{\star}\boxed{\star\star}$$

$$\binom{7+2}{7} = \frac{9!}{7!(9-7)!} = 36.$$

De forma geral, se t é o número total de pontos da série temporal e se s sua soma, então o número de possíveis séries temporais para o adversário decidir a correta é determinado por s mais $t-1$ escolhendo s, portanto

$$\binom{s+t-1}{s} = \frac{(s+t-1)!}{(t-1)!s!} = \binom{s+t-1}{i-1}. \qquad (1)$$

Tópicos

Ruído

[Oli17a]

Suponha que $\mathfrak{M}_{i,j} = m_{i,j} + r_{i,j}$ é a mensagem $m_{i,j}$ com ruído $r_{i,j}$ de usuário i no tempo j. Por simplicidade, suponha que a distribuição tenha valor esperado $\mu = 0$, logo a série de ruídos converge para zero

$$\sum_{i}^{\infty} r_{i,j} = \sum_{j}^{\infty} r_{i,j} \to 0.$$

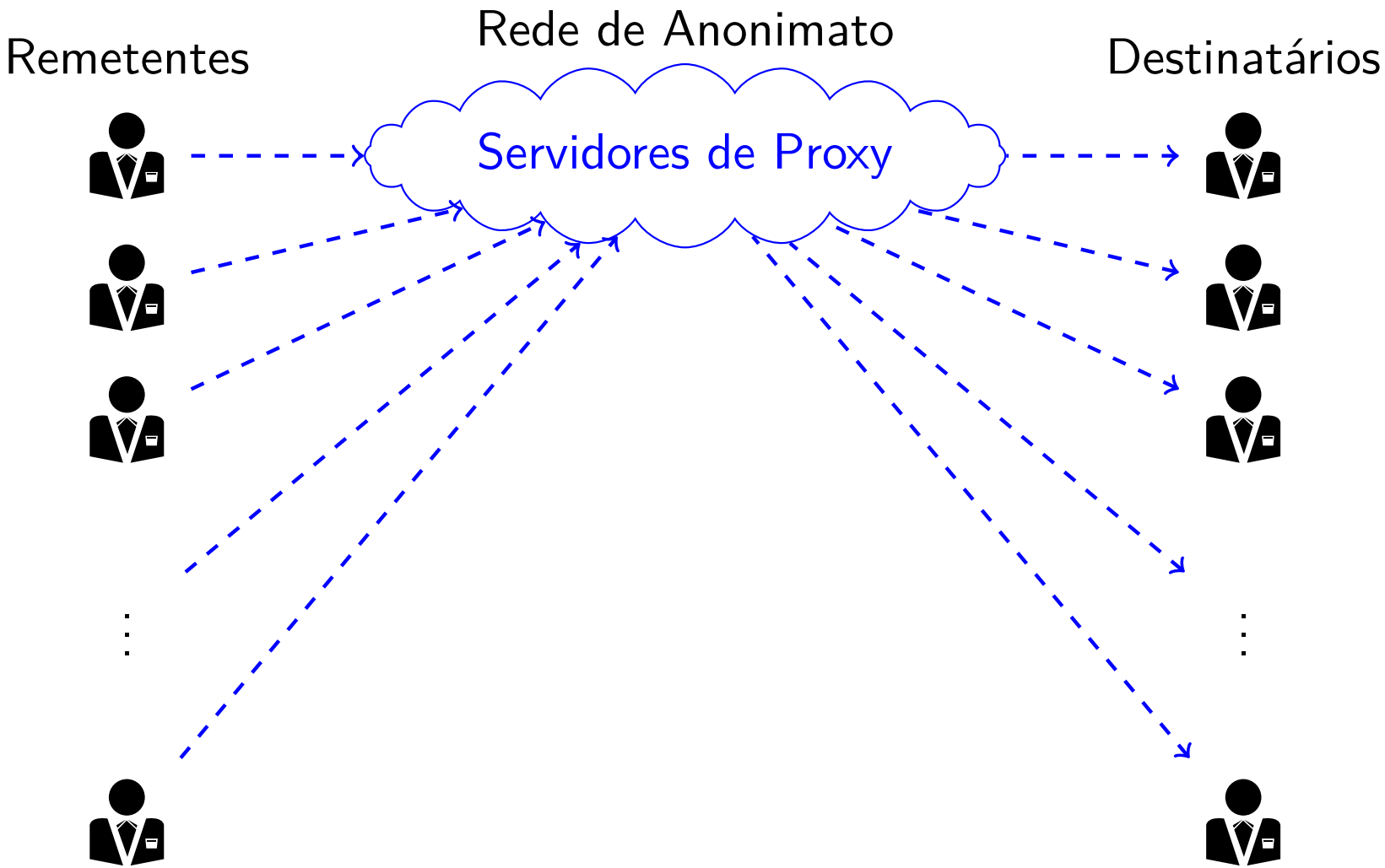
Desta forma, um adversário gera uma série de ruídos r'_l com a mesma distribuição e computa

$$\mathfrak{M}_{i,j} + \sum_{l=1}^{L} r'_l \to m_{i,j},$$

onde L é um número suficientemente grande.

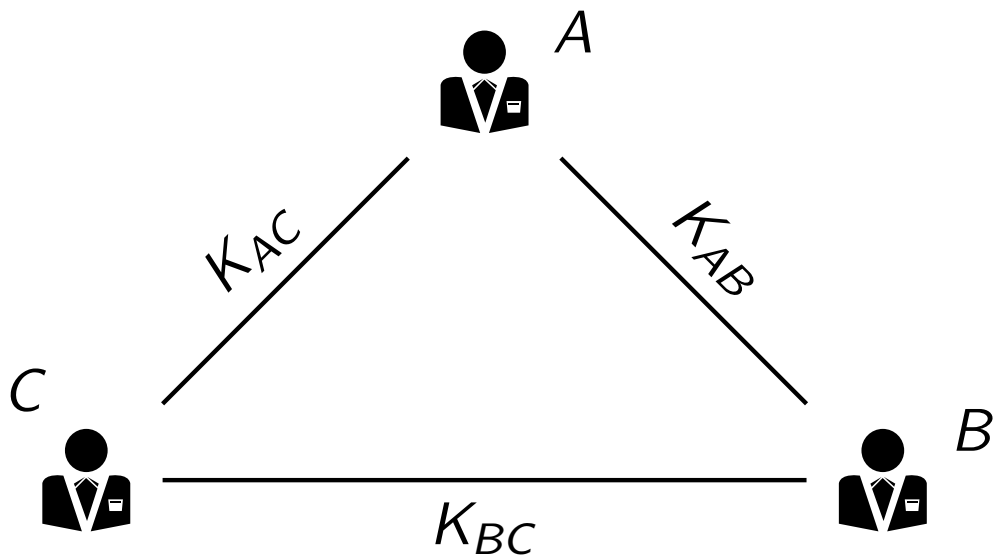
Pseudônimo e Redes de Anonimato

[Cha81]



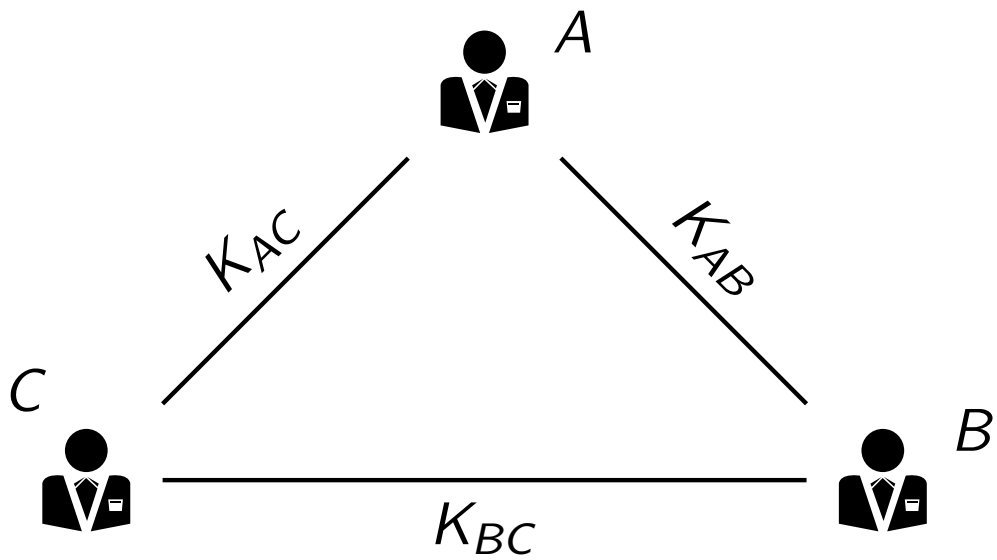
DC-Net simétrica (SDC-Net)

[Cha88] - Dining Cryptographers Problem



SDC-Net

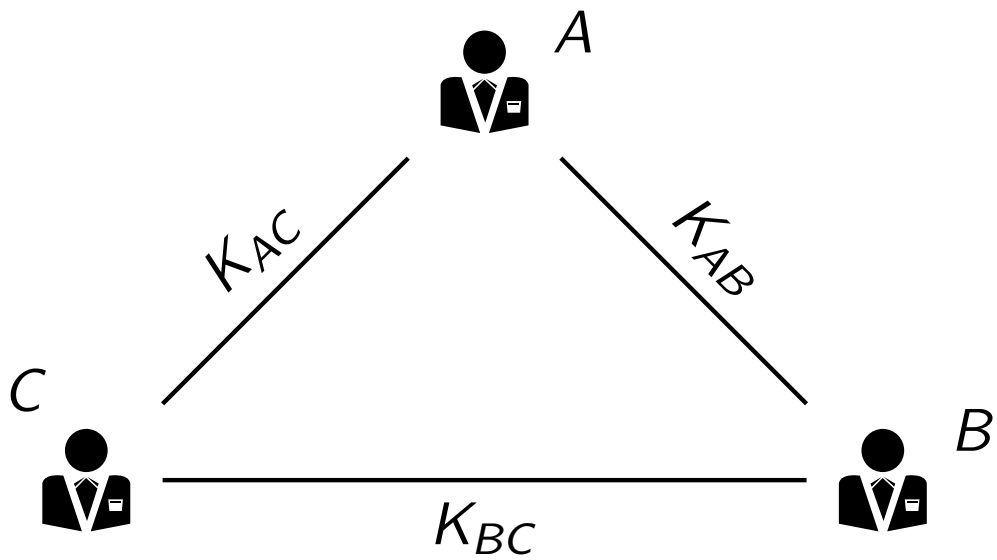
[Cha88] - Dining Cryptographers Problem



$$K_{AB} \oplus K_{AC} \oplus 1 \oplus K_{AB} \oplus K_{BC} \oplus K_{AC} \oplus K_{BC} = 1.$$

SDC-Net

[Cha88] - Dining Cryptographers Problem



$$K_{AB} \oplus K_{AC} \oplus 1 \oplus K_{AB} \oplus K_{BC} \oplus K_{AC} \oplus K_{BC} = 1.$$

$$K_{AB} \oplus K_{AC} \oplus K_{AB} \oplus K_{BC} \oplus K_{AC} \oplus K_{BC} = 0.$$

A é um adversário

Que enviou 1

$$K_{AB} \oplus \underbrace{(K_{AB} \oplus K_{BC})}_{\text{revelado por } B} = K_{BC}$$

e

$$K_{Ac} \oplus \underbrace{(K_{AC} \oplus K_{BC})}_{\text{revelado por } C} = K_{BC}.$$

A é um adversário

Que enviou 1

$$K_{AB} \oplus \underbrace{(K_{AB} \oplus K_{BC})}_{\text{revelado por } B} = K_{BC}$$

e

$$K_{Ac} \oplus \underbrace{(K_{AC} \oplus K_{BC})}_{\text{revelado por } C} = K_{BC}.$$

Atenção

A chave só pode ser usada uma vez!

A é um adversário

Obejetivo: descobrir quem enviou 1

Se A não tivesse enviado a mensagem que pagou, ou A teria obtido

$$K_{AB} \oplus \underbrace{(K_{AB} \oplus K_{BC} \oplus 1)}_{\text{revelado por } B} = K_{BC} \oplus 1$$

e

$$K_{Ac} \oplus \underbrace{(K_{AC} \oplus K_{BC})}_{\text{revelado por } C} = K_{BC},$$

ou A teria obtido

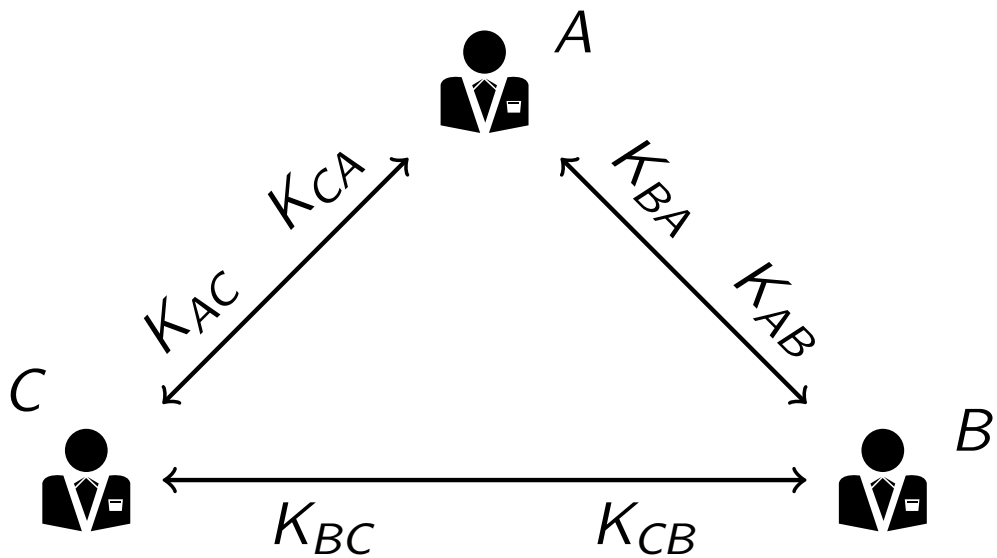
$$K_{AB} \oplus \underbrace{(K_{AB} \oplus K_{BC})}_{\text{revelado por } B} = K_{BC}$$

e

$$K_{Ac} \oplus \underbrace{(K_{AC} \oplus K_{BC} \oplus 1)}_{\text{revelado por } C} = K_{BC} \oplus 1.$$

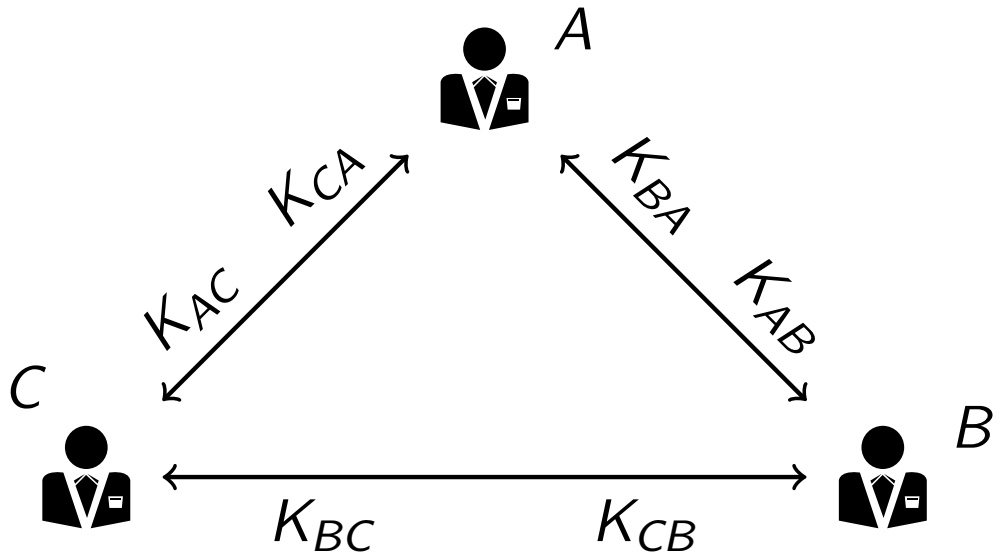
SDC-Net

Dígrafo completo



SDC-Net

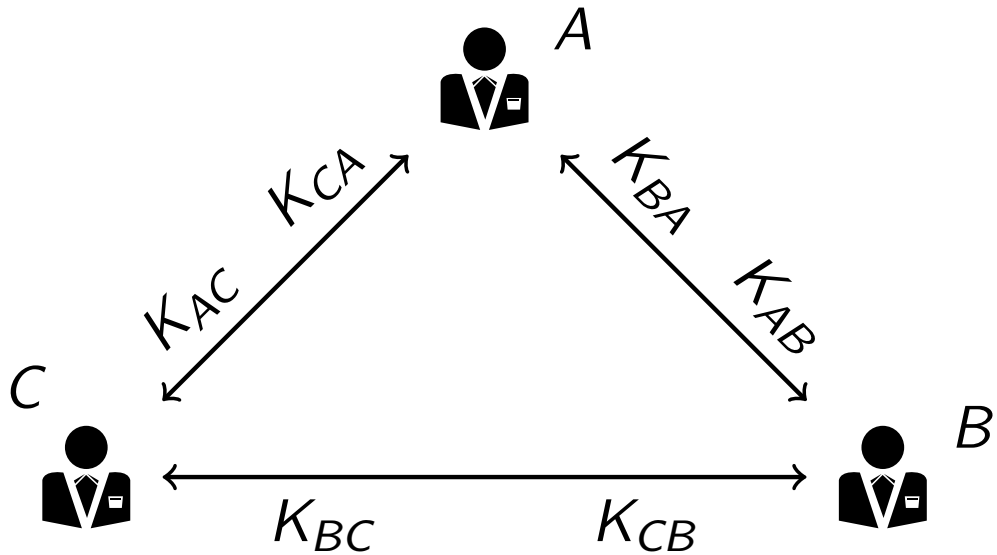
Dígrafo completo



$$\mathfrak{M}_{i,j} = m_{i,j} + \sum_{o \in \mathcal{U} - \{i\}} \mathrm{H}\left(k_{i,o} || j\right) - \mathrm{H}\left(k_{o,i} || j\right),$$

SDC-Net

Dígrafo completo



$$\mathfrak{M}_{i,j} = m_{i,j} + \sum_{o \in \mathcal{U} - \{i\}} \mathrm{H}\left(k_{i,o} || j\right) - \mathrm{H}\left(k_{o,i} || j\right),$$

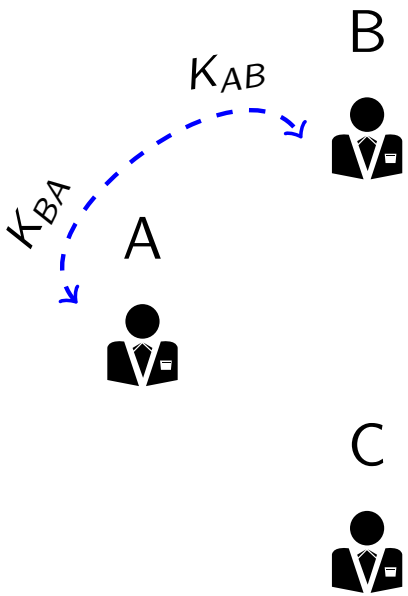
$$c_j = \sum_{i=1}^{I} \mathfrak{M}_{i,j}.$$

SDC-Nets

[Cha88]

SDC-Nets

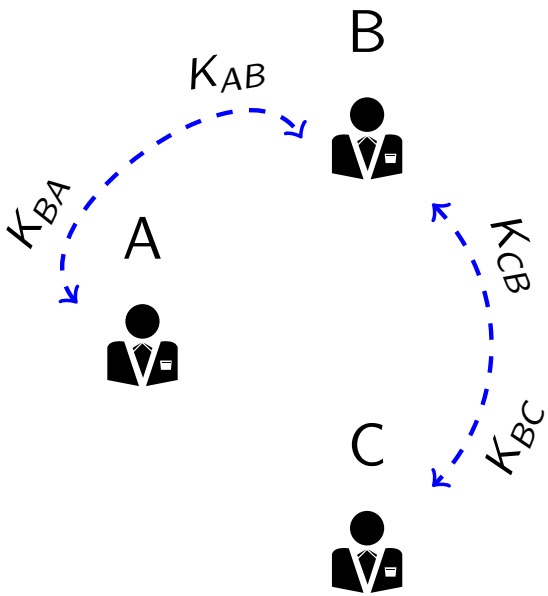
[Cha88]



Contador

SDC-Nets

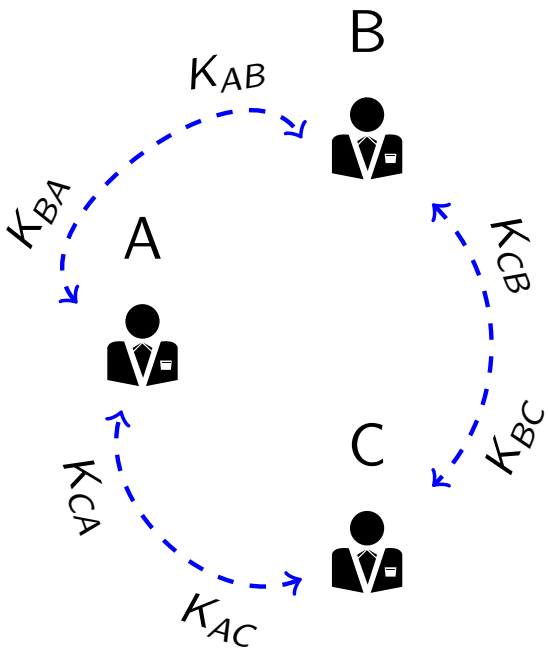
[Cha88]



Contador

SDC-Nets

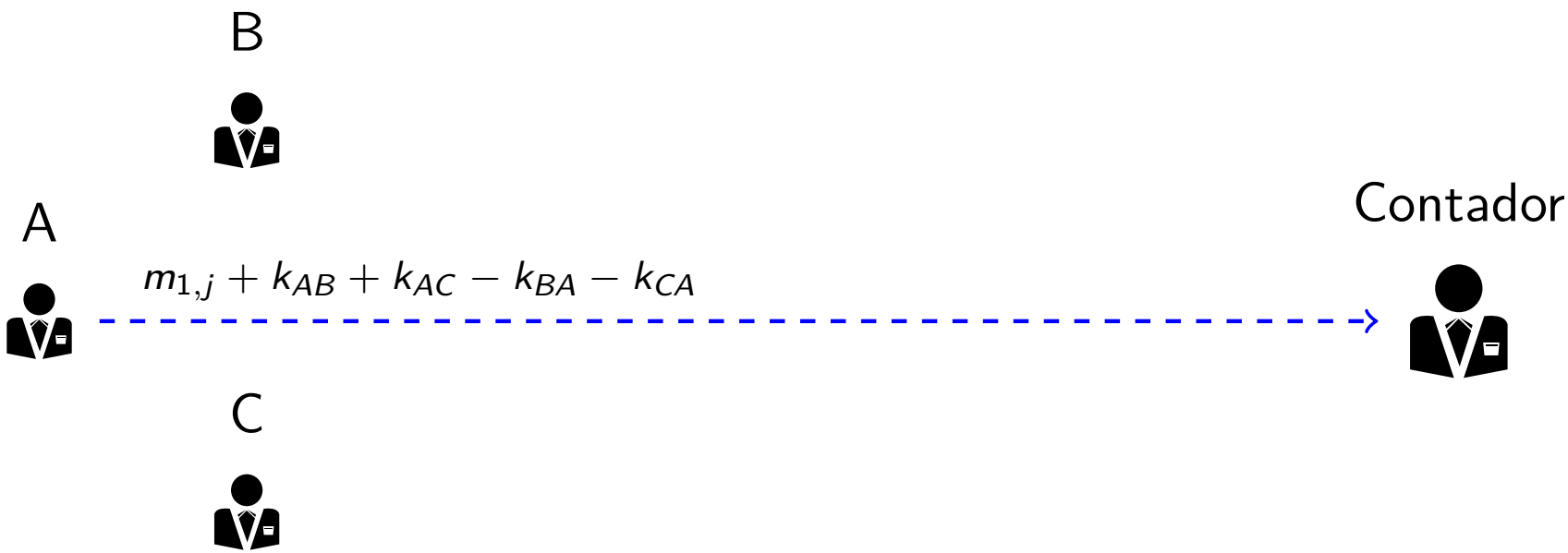
[Cha88]



Contador

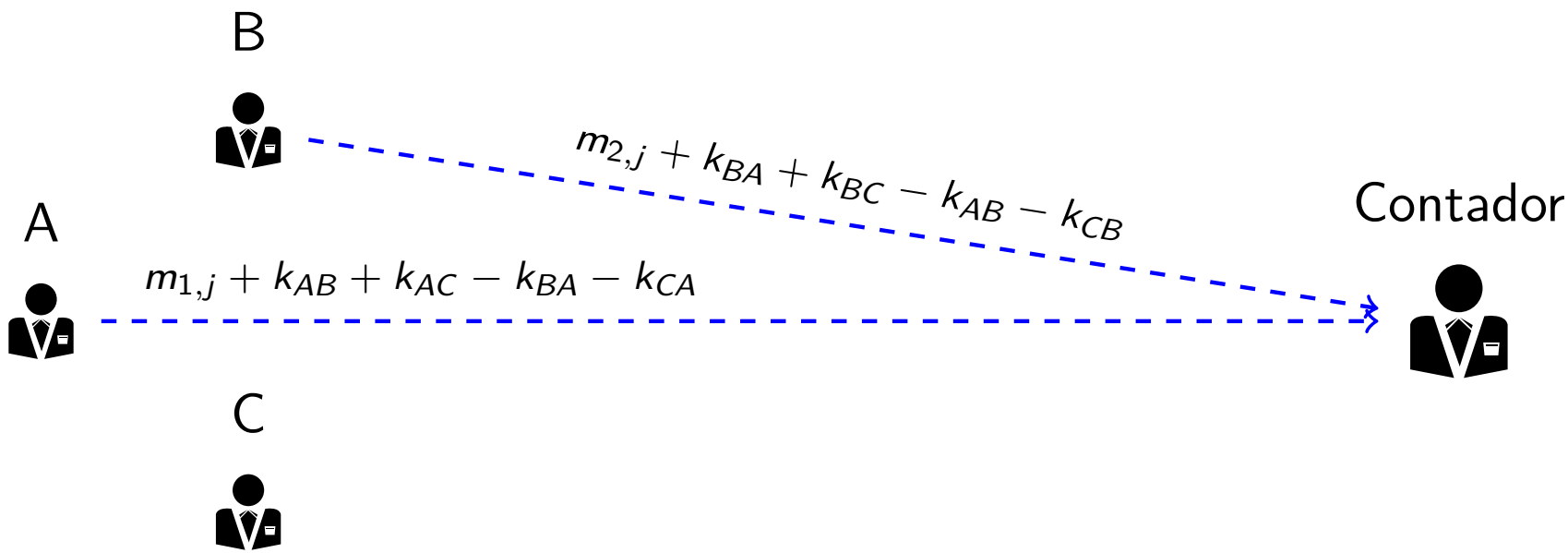
SDC-Nets

Unconditional Secure [Cha88]



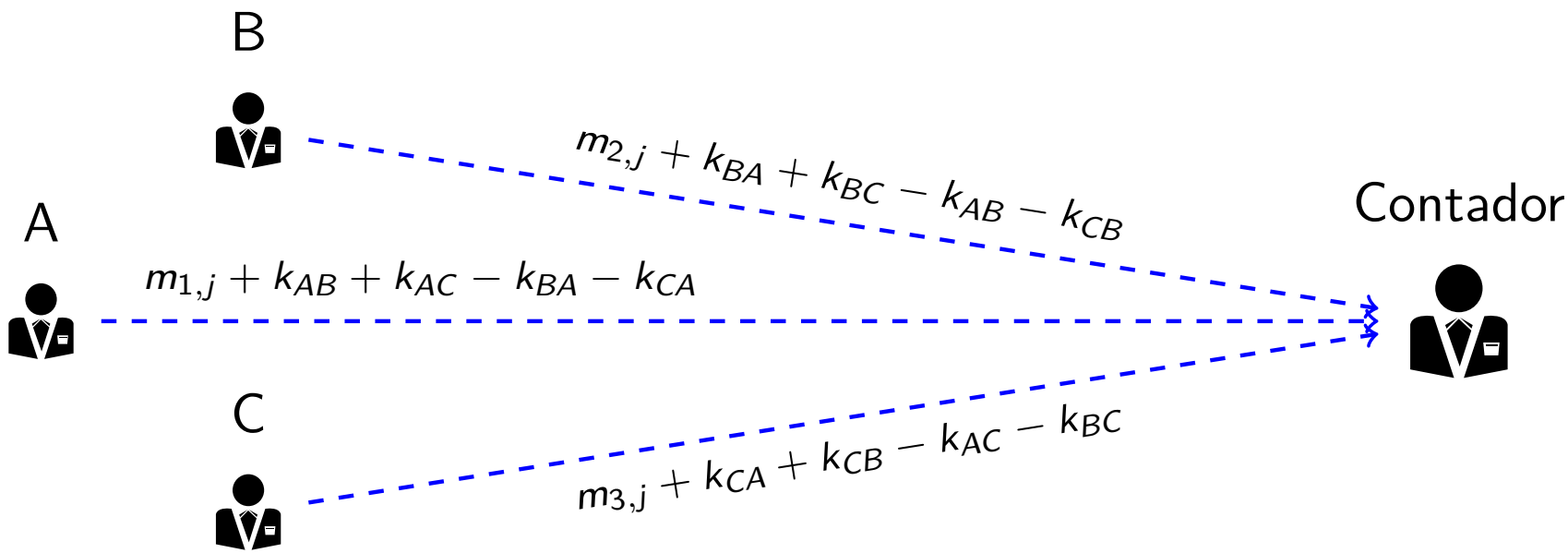
SDC-Nets

Unconditional Secure [Cha88]



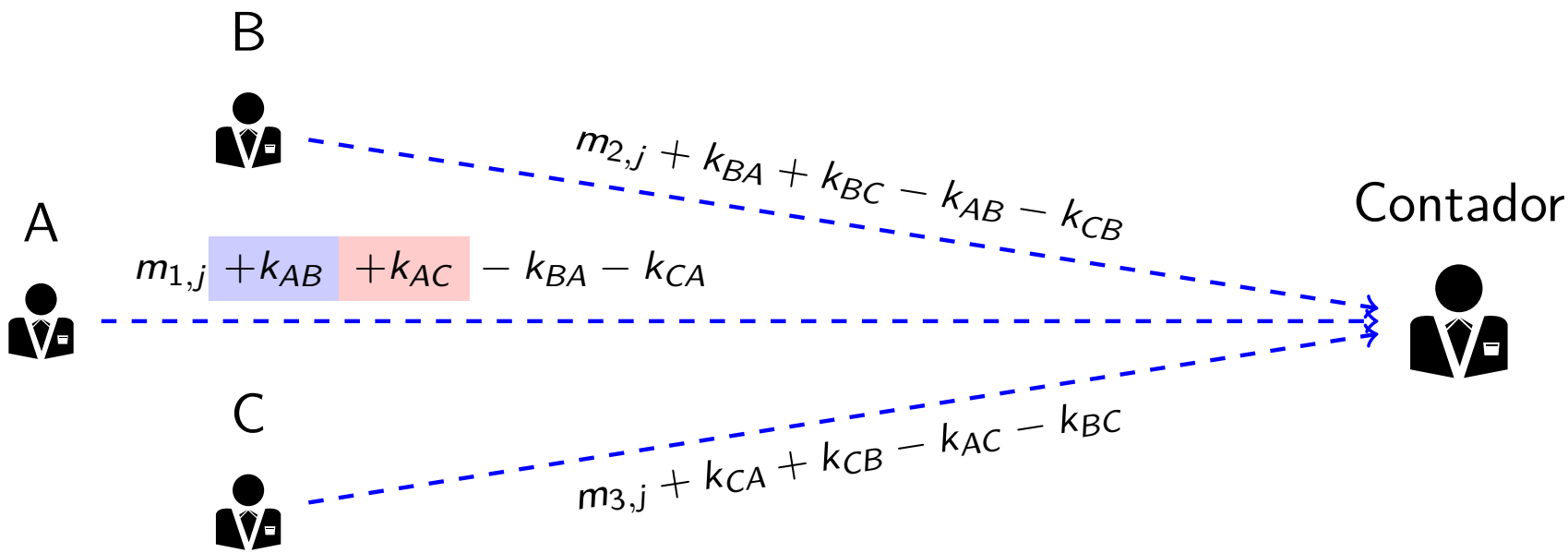
SDC-Nets

Unconditional Secure [Cha88]



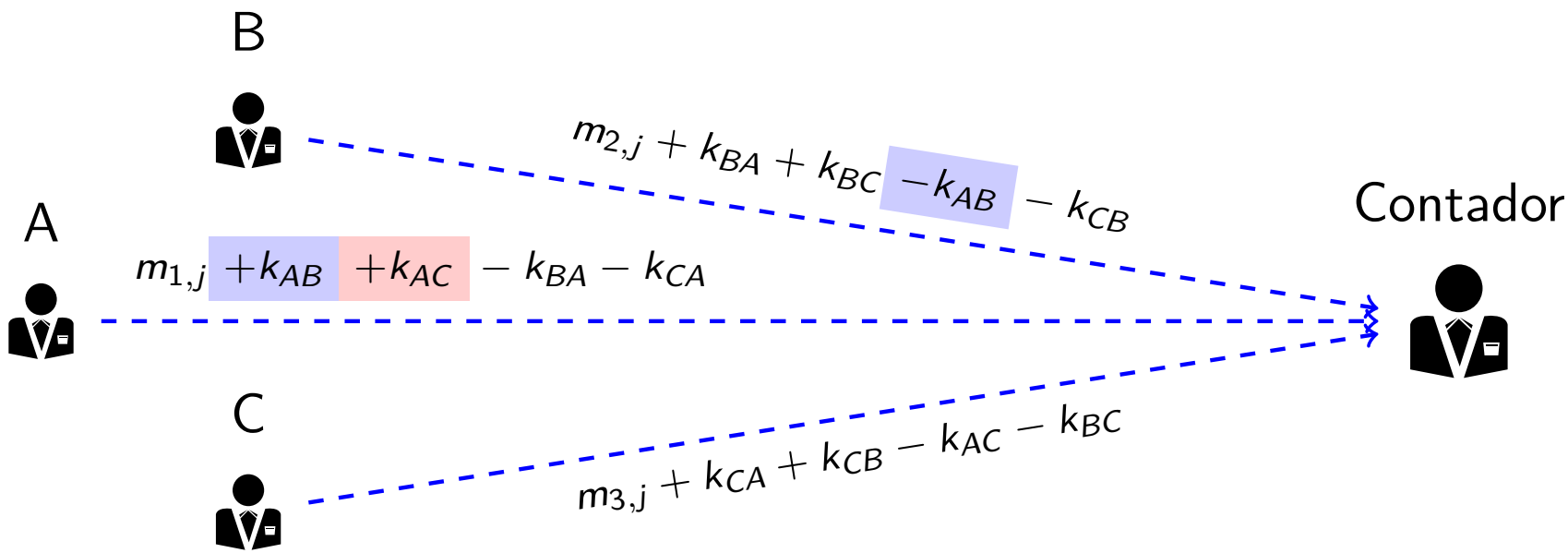
SDC-Nets

Unconditional Secure [Cha88]



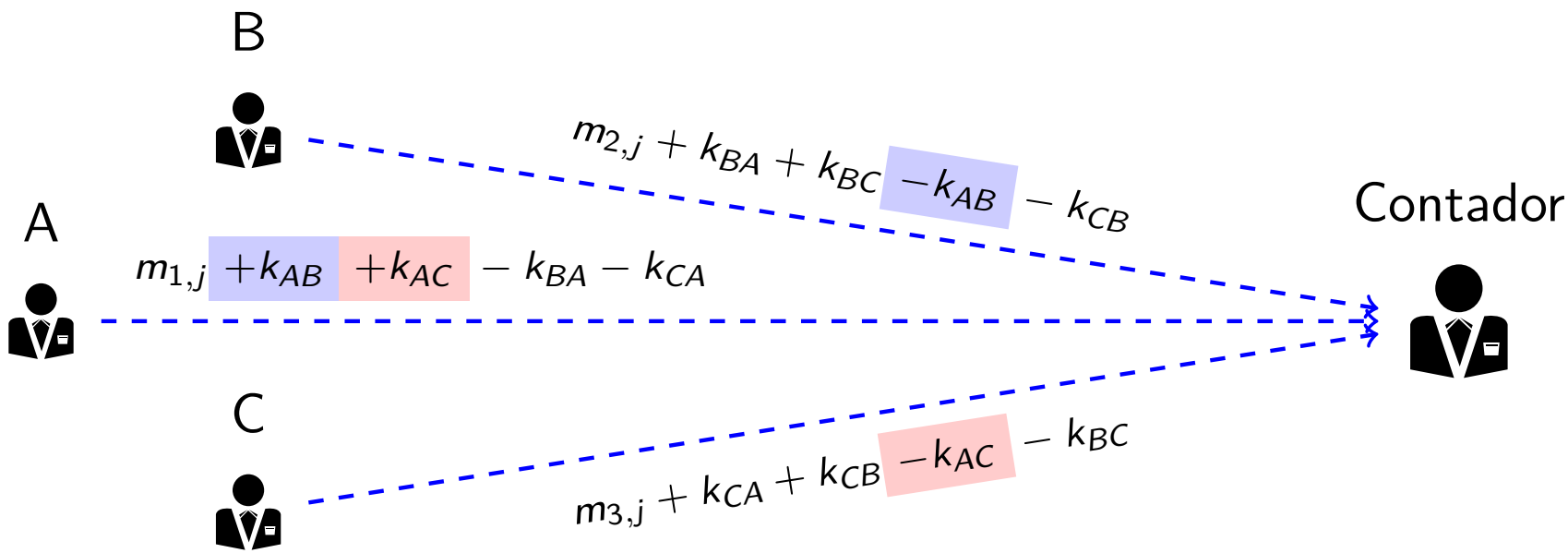
SDC-Nets

Unconditional Secure [Cha88]



SDC-Nets

Unconditional Secure [Cha88]

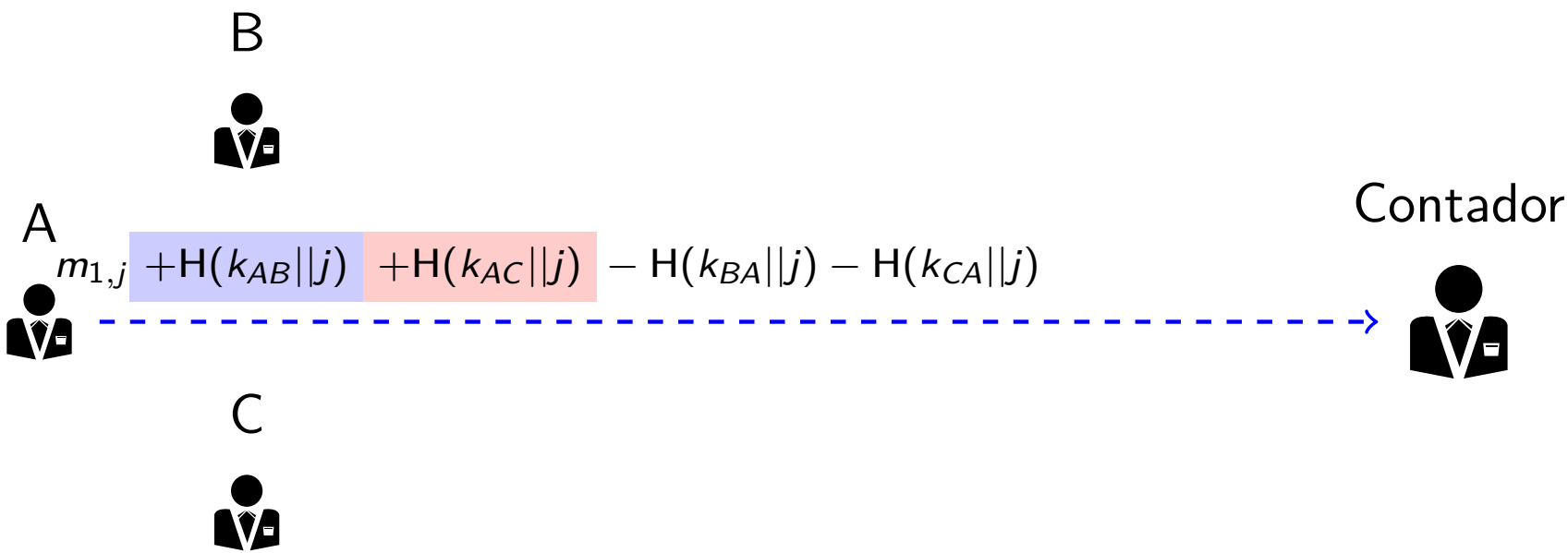


SDC-Nets

[Golle2004]

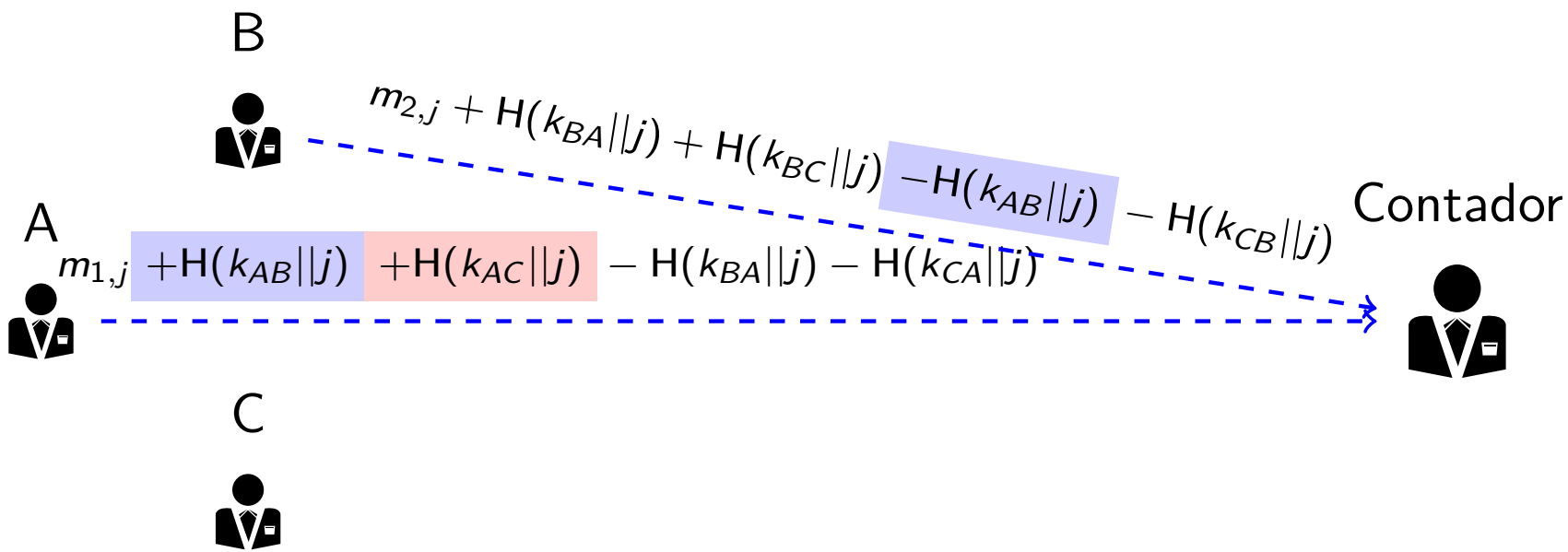
SDC-Nets

[Golle2004]



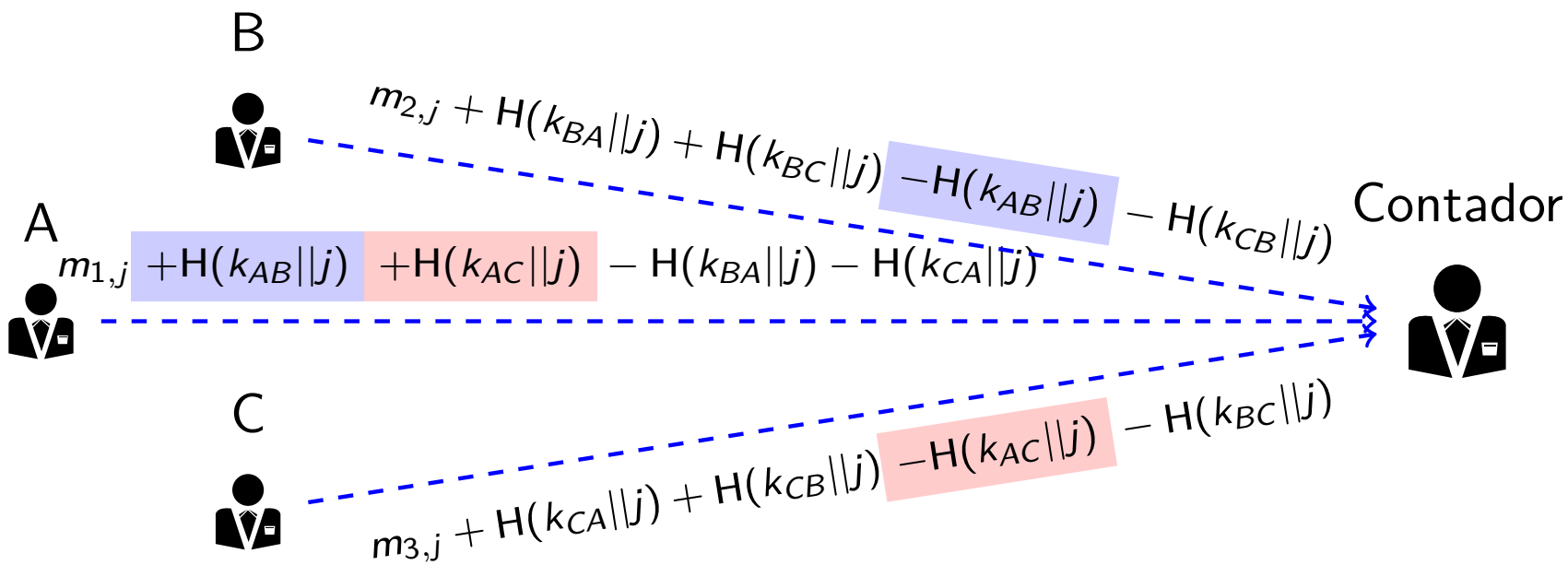
SDC-Nets

[Golle2004]



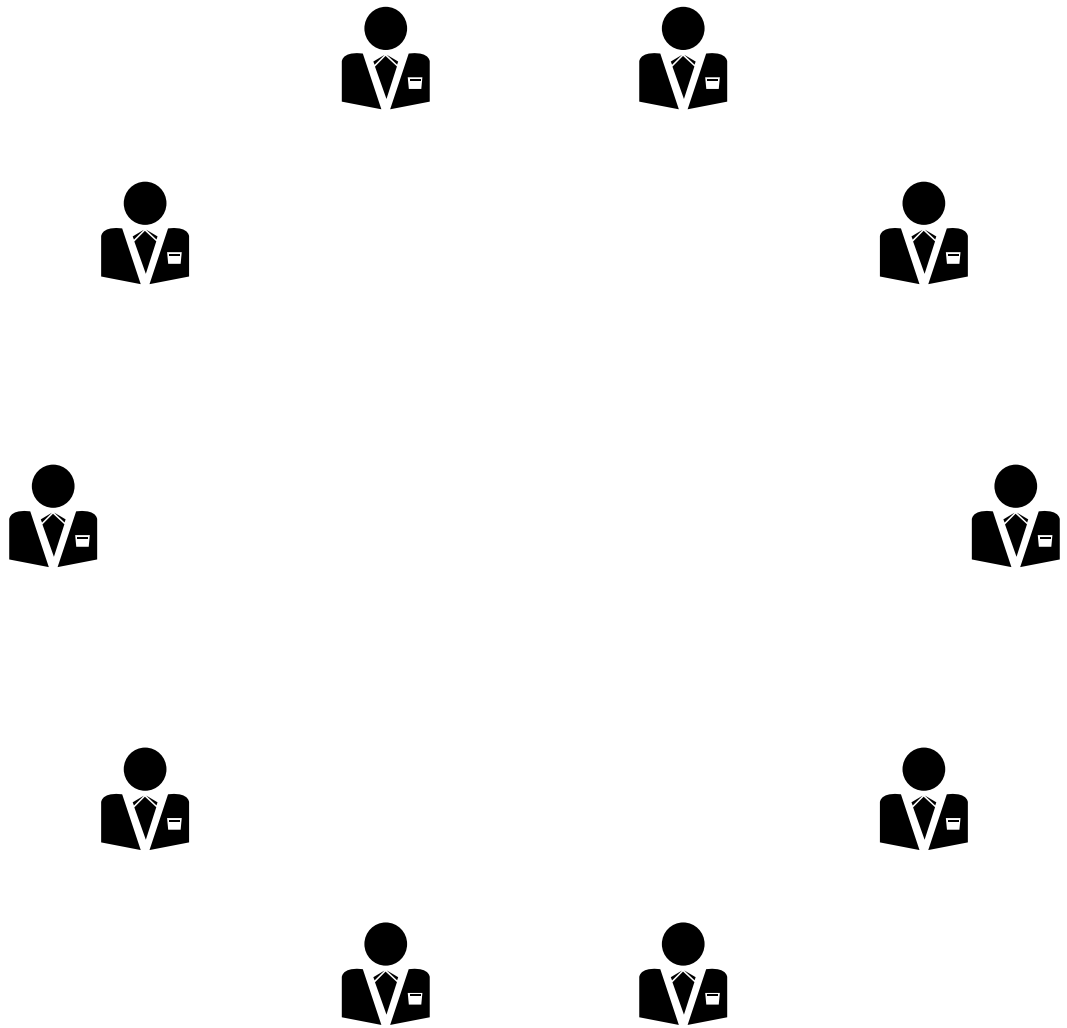
SDC-Nets

[Golle2004]



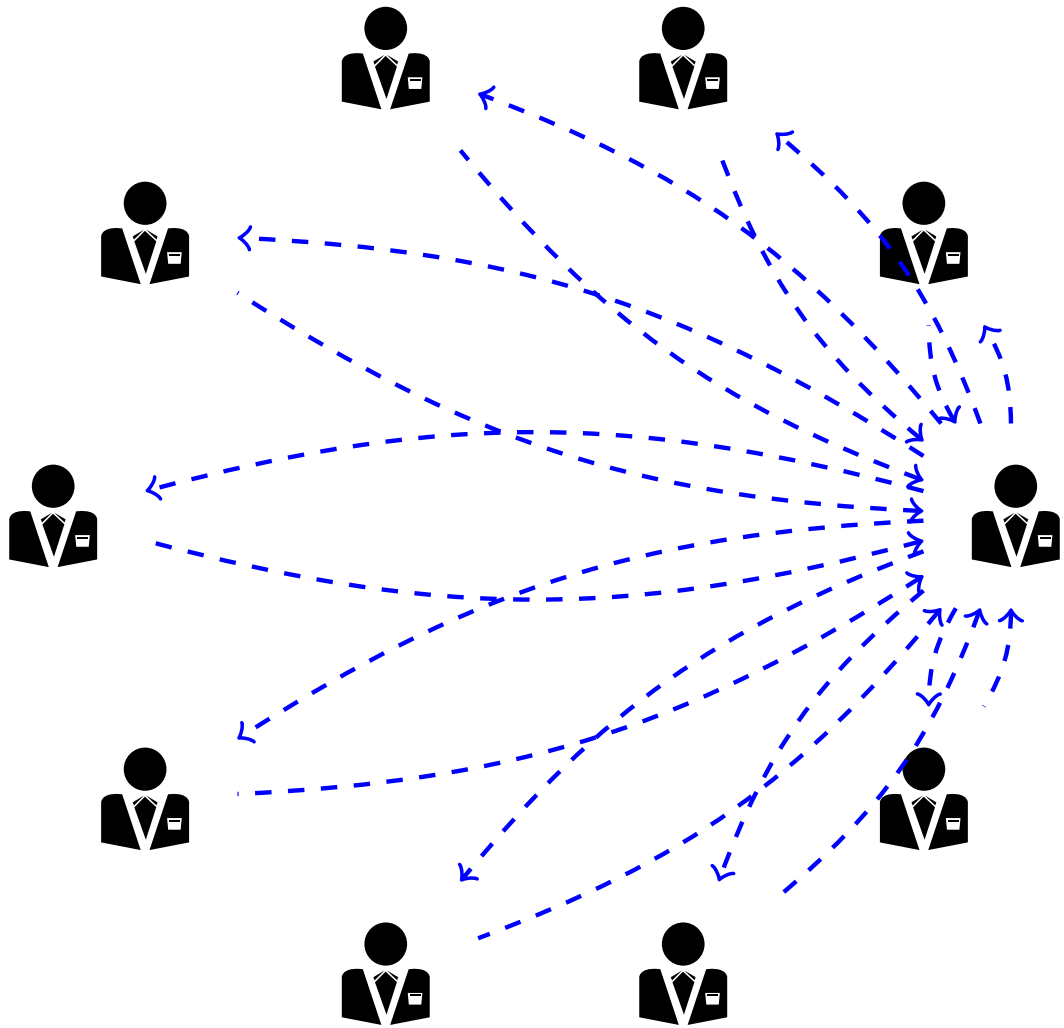
SDC-Net

Chaves para 10 usuários



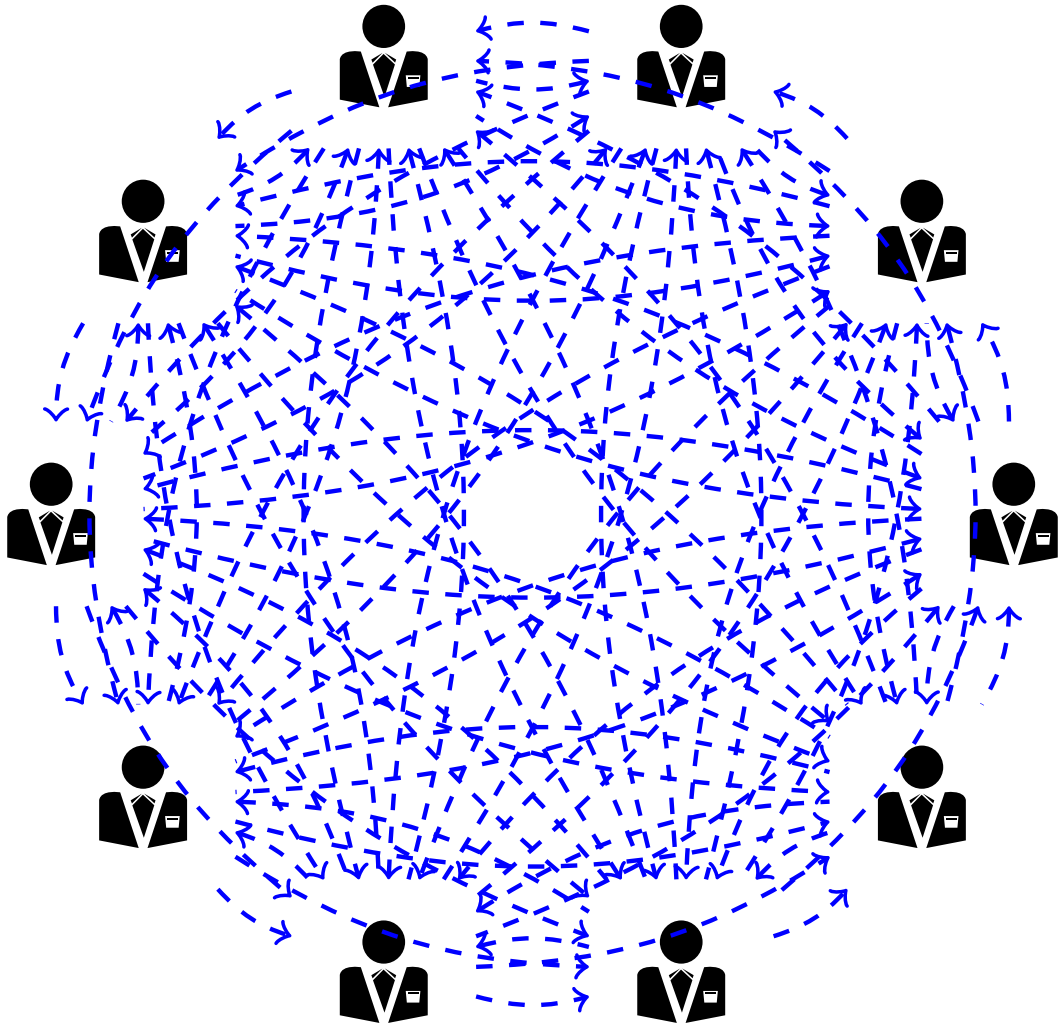
SDC-Net

Chaves para 10 usuários



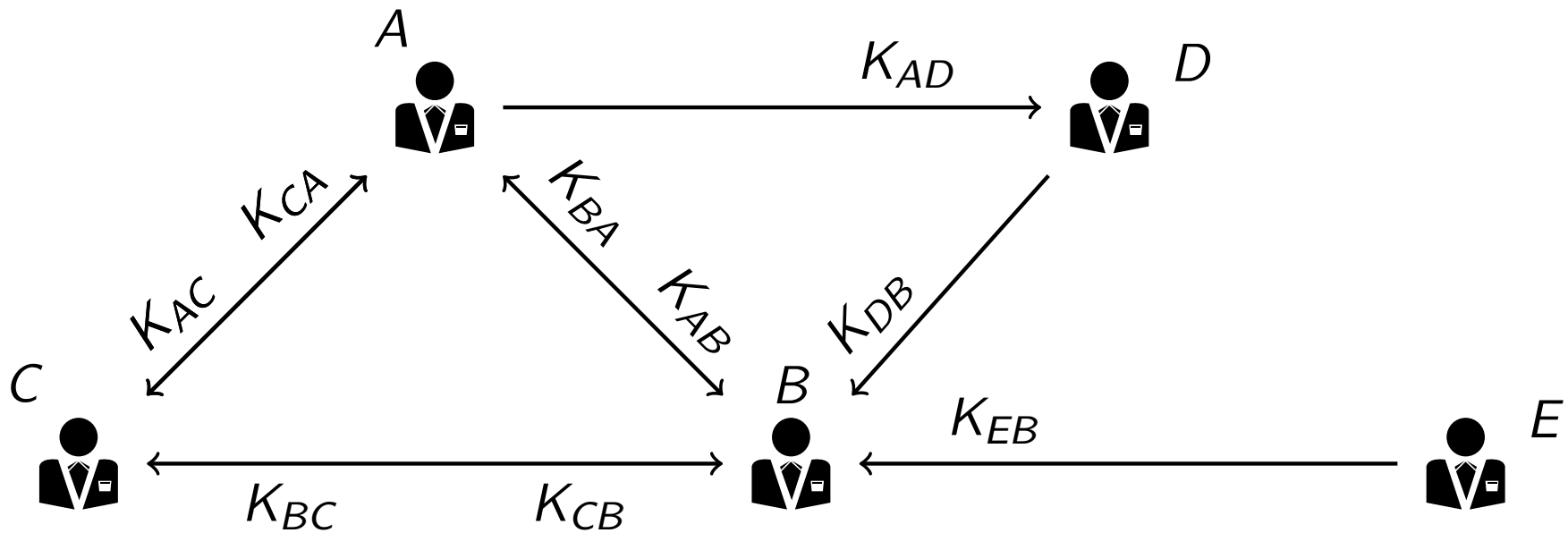
SDC-Net

Chaves para 10 usuários



SDC-Net

Conceito de usuários confiáveis



Problemas de usar SDC-Net

Ruptura

Um usuário pode enviar um valor inverso ou gigante.

Problemas de usar SDC-Net

Ruptura

Um usuário pode enviar um valor inverso ou gigante.

Crescimento do número de chaves

$$\frac{I(I-1)}{2}.$$

Tópicos

Compromisso (Commitment)

$$\mathfrak{N}_{i,j} = \mathsf{Commit}(m_{i,j}, \mathfrak{v}_{i,j})$$

e

$$\mathsf{Open}(\mathfrak{N}_{i,j}, m_{i,j}, \mathfrak{v}_{i,j}) = \top \veebar \bot$$

Compromisso (Commitment)

$$\mathfrak{N}_{i,j} = \text{Commit}(m_{i,j}, \mathfrak{v}_{i,j})$$

e

$$\text{Open}(\mathfrak{N}_{i,j}, m_{i,j}, \mathfrak{v}_{i,j}) = \top \veebar \bot$$

Atenção

Commit não é uma função que encripta e Open não decripta.

Verificação

Auditor

$$\mathfrak{N}_{i,j} = \text{Commit}(m_{i,j}, \mathfrak{v}_{i,j})$$

e manda $\mathfrak{N}_{i,j}$ o resultado para um auditor. O auditor calcula

$$\mathfrak{U}_i = \prod_{j=1}^{J} \mathfrak{N}_{i,j}$$

enquanto cada usuário calcula

$$b_i = \sum_{j=1}^{J} m_{i,j}$$

e

$$\mathfrak{V}_i = \sum_{j=1}^{J} \mathfrak{v}_{i,j}$$

e envia $\mathfrak{U}_i$ e $\mathfrak{V}_i$ para o auditor.

Verificação

Auditor

O auditor verifica b_i e o usuário i prova, calculando

$$\text{Open}\left(\mathfrak{U}_i, b_i, \mathfrak{V}_i\right) = \top \veebar \bot.$$

Verificação

Auditor

O auditor verifica b_i e o usuário i prova, calculando

$$\text{Open}\left(\mathfrak{U}_i, b_i, \mathfrak{V}_i\right) = \top \veebar \bot.$$

Se o auditor quisesse verificar a consolidação c_j, bastaria calcular

$$\mathfrak{T}_j = \prod_{i=1}^{I} \mathfrak{N}_{i,j}$$

e pedir o verificador no tempo j

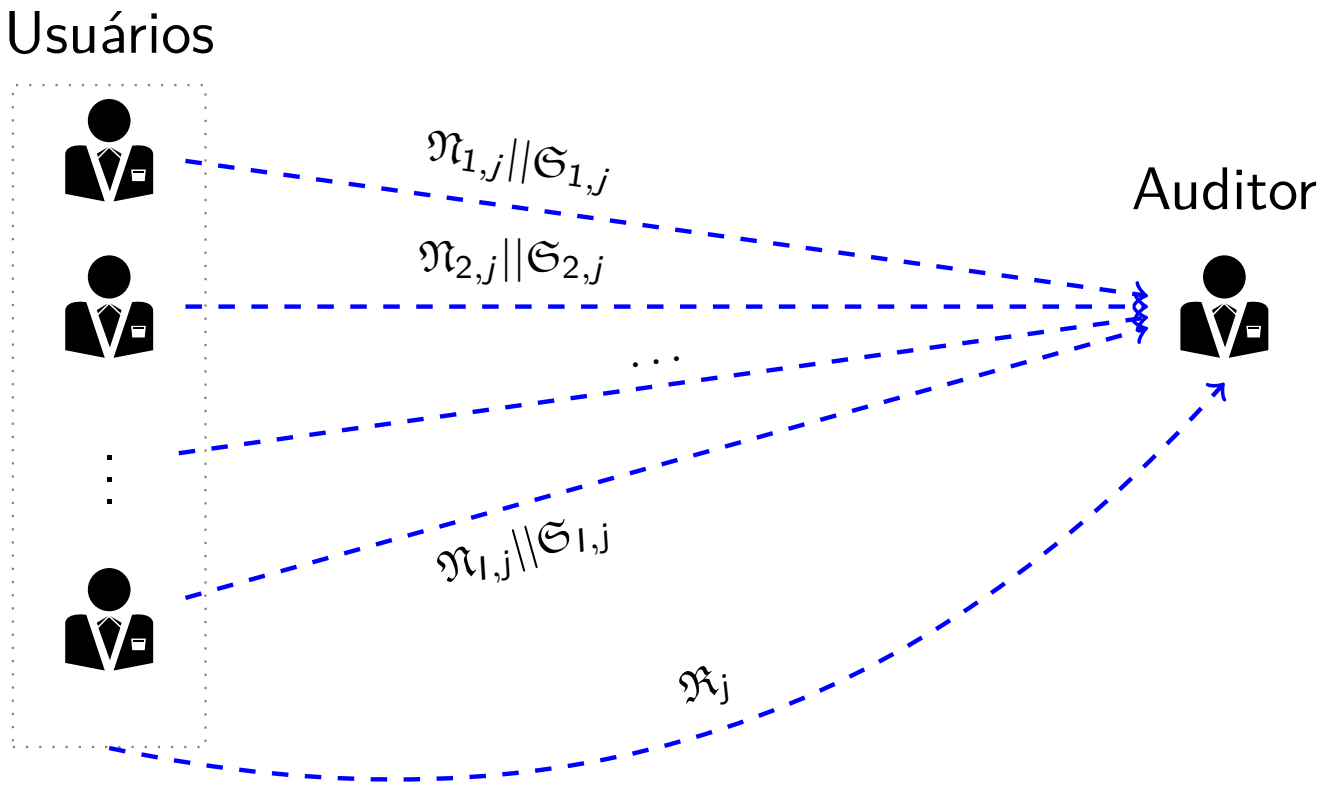
$$\mathfrak{R}_j = \sum_{i=1}^{I} \mathfrak{v}_{i,j}.$$

Os usuários poderiam calcular o verificar com uma SDC-Net. Com as informações, o auditor verifica se

$$\text{Open}\left(\mathfrak{T}_j, c_j, \mathfrak{R}_j\right) = \top \veebar \bot.$$

Assinatura

Cada mensagem comprometida $\mathfrak{N}_{i,j} = \text{Commit}(m_{i,j}, \mathfrak{v}_{i,j})$ deve ir concatenada a sua respectiva assinatura digital $\mathfrak{S}_{i,j} = \text{Sign}\left(\mathfrak{N}_{i,j}\right)$.



Incondicional

[Ped92]

Eles escolhem dois primos grandes p e q tal que $q|(p-1)$ e um gerador g de ordem q. Cada usuário escolhe secretamente um $a_i \in \mathbb{Z}_q$ e calcula

$$h_i = g^{a_i} \pmod{p}$$

depois envia h_1 para o auditor.

Incondicional

[Ped92]

Eles escolhem dois primos grandes p e q tal que $q|(p-1)$ e um gerador g de ordem q. Cada usuário escolhe secretamente um $a_i \in \mathbb{Z}_q$ e calcula

$$h_i = g^{a_i} \pmod{p}$$

depois envia h_1 para o auditor.

Nota

Note que dado h_i, g, e p, não se sabe da existência de um algoritmo clássico com tempo polinomial que determine a_i.

Incondicional

[Ped92]

Eles escolhem dois primos grandes p e q tal que $q|(p-1)$ e um gerador g de ordem q. Cada usuário escolhe secretamente um $a_i \in \mathbb{Z}_q$ e calcula

$$h_i = g^{a_i} \pmod{p}$$

depois envia h_1 para o auditor.

Nota

Note que dado h_i, g, e p, não se sabe da existência de um algoritmo clássico com tempo polinomial que determine a_i.

Para enviar a mensagem comprometida $\mathfrak{N}_{i,j}$, os usuários escolhem aleatoriamente outro valor secreto $\mathfrak{v}_{i,j} \in \mathbb{Z}_q$ e calculam

$$\mathfrak{N}_{i,j} = \text{Commit}\left(m_{i,j}, \mathfrak{v}_{i,j}\right) = g^{m_{i,j}} h_i^{\mathfrak{v}_{i,j}} \mod p,$$

onde $m_{i,j} \in \mathbb{Z}_q$.

Verificação

$$\mathfrak{U}_i = \prod_{j=1}^{J} \mathfrak{N}_{i,j} = \prod_{j=1}^{J} g^{m_{i,j}} h_i^{\mathfrak{v}_{i,j}} \mod p$$

enquanto o usuário i calcula

$$b_i = \sum_{j=1}^{J} m_{i,j}$$

e

$$\mathfrak{V}_i = \sum_{j=1}^{J} \mathfrak{v}_{i,j}.$$

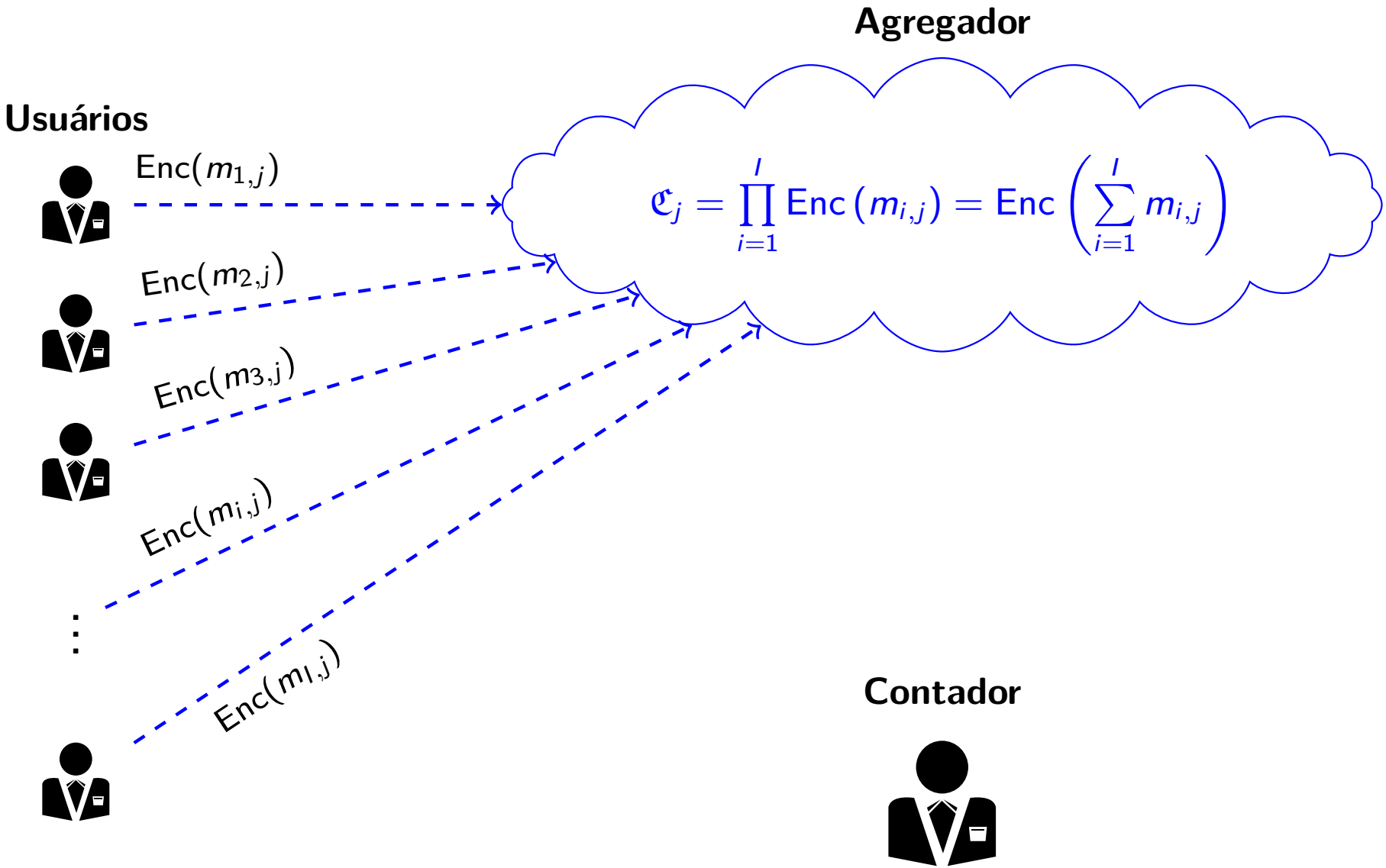
O usuário i envia $\mathfrak{U}_i$ e $\mathfrak{V}_i$ para o auditor que calcula

$$\text{Open}\left(\mathfrak{U}_i, b_i, \mathfrak{V}_i\right) = \left(\mathfrak{U}_i \stackrel{?}{=} g^{b_i} h_i^{\mathfrak{V}_i} \mod p\right)$$

e verifiquem se o resultado é verdadeiro $\top$ ou se é falso $\bot$.

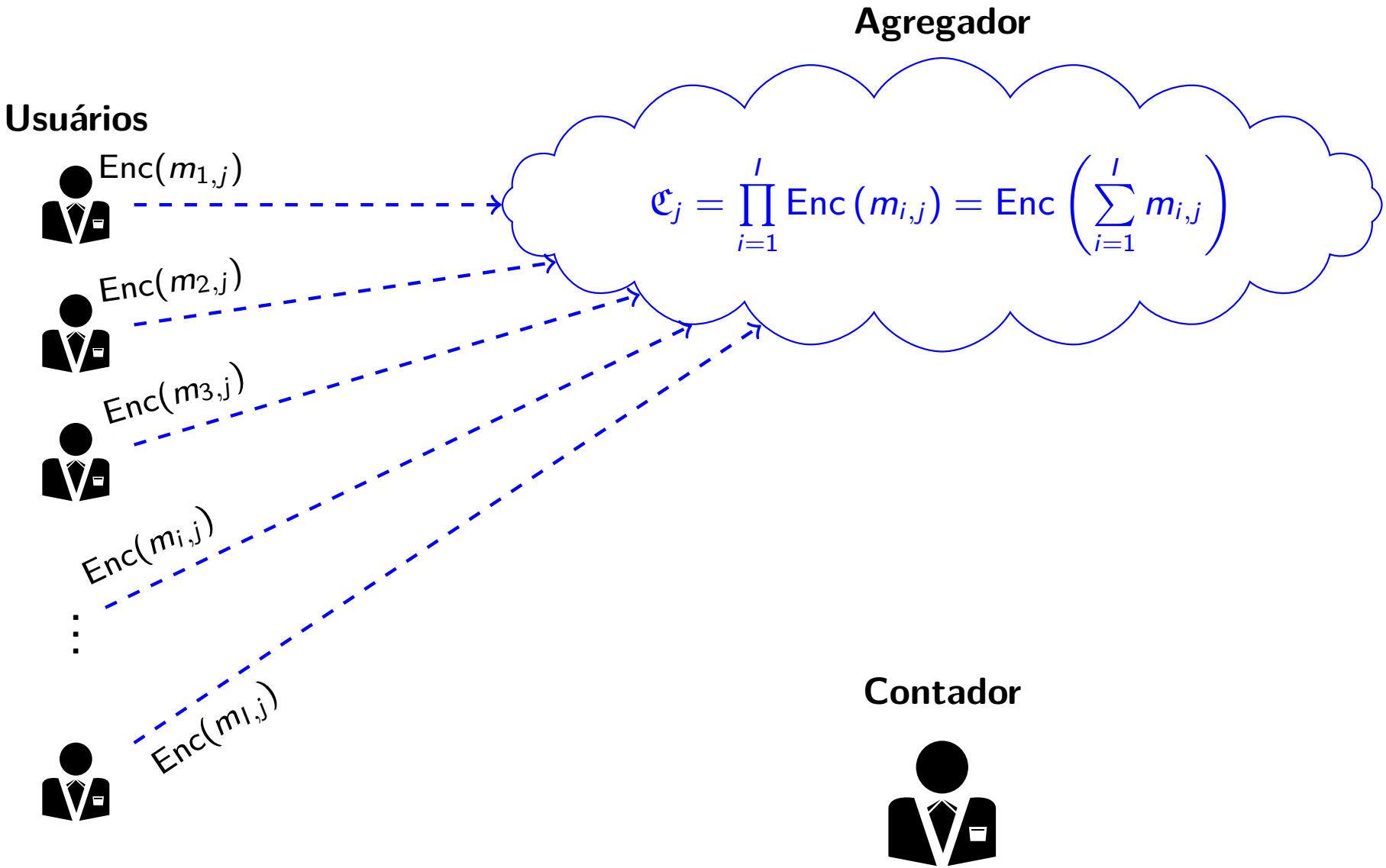
Agregação

Primitiva de criptografia homomórfica aditivas (PCHAs)



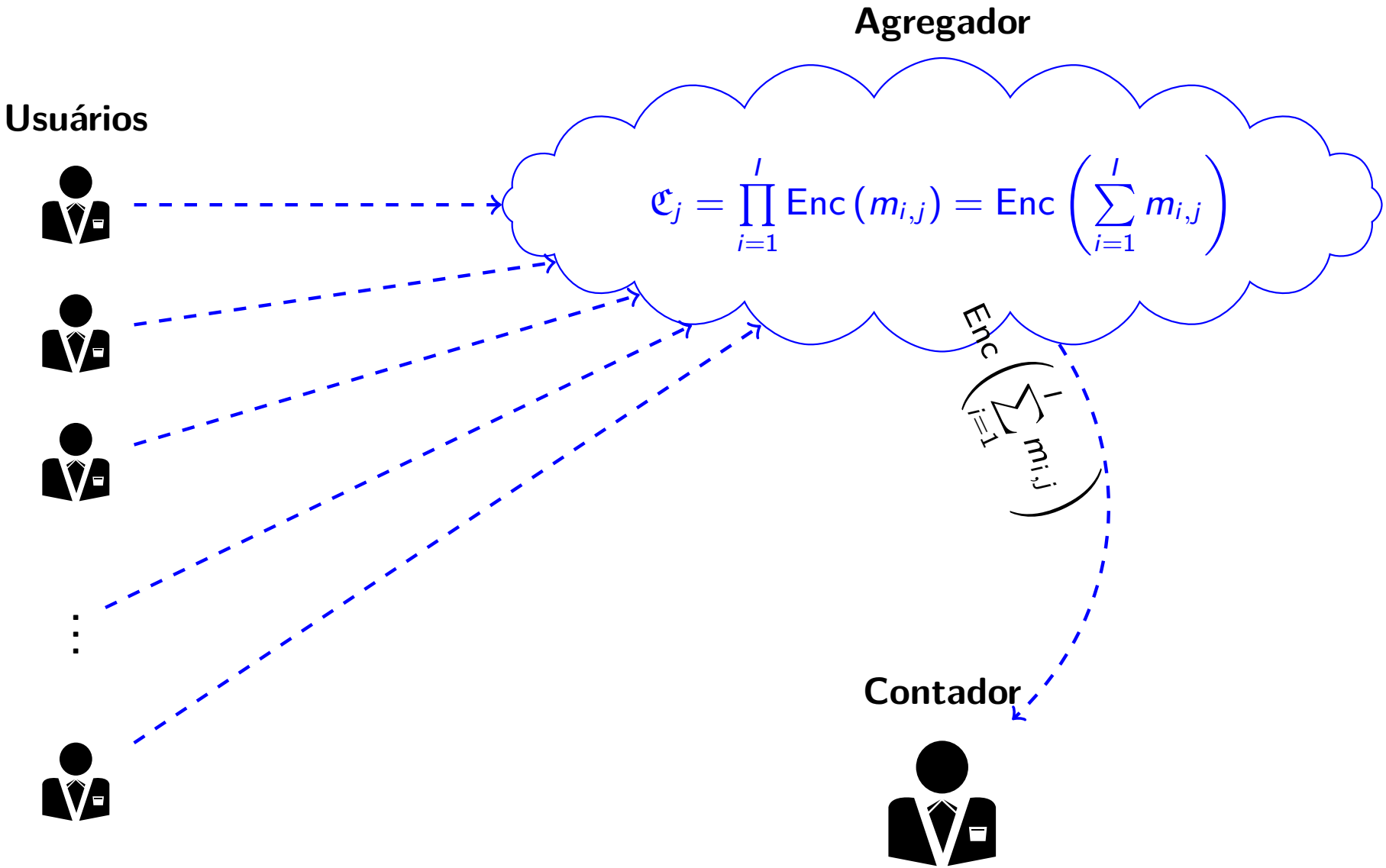
Agregação

PCHAs



Agregação

PCHAs



Encriptação Homomórfica Aditiva

[Pai99]

O contador calcula $n = p \cdot q$ e $\lambda = \text{mmc}(p-1, q-1)$, e escolhe $g \in \mathbb{Z}^*_{n^2}$ tal que n divide a ordem de g. O contador tem a chave privada (λ, μ) e distribui a chave pública (n, g).

$$\text{Enc} : \mathbb{Z}_n \times \mathbb{Z}^*_n \to \mathbb{Z}_{n^2}$$

$$\text{Enc}(m_{i,j}, r_{i,j}) \mapsto g^{m_{i,j}} \cdot \mathfrak{v}_{i,j}{}^n \mod n^2,$$

onde $\mathfrak{v}_{i,j}$ é um valor randômico secreto. Agregador calcula

$$\mathfrak{C}_j = \sum_{i=1}^{I} \mathfrak{M}_{i,j}.$$

Para descriptografar o contador aplica a função

$$\text{Dec} : \mathbb{Z}_{n^2} \to \mathbb{Z}_n$$

$$\text{Dec}(\mathfrak{C}_j) \mapsto \text{L}(\mathfrak{C}_j{}^{\lambda} \mod n^2) \cdot d \mod n,$$

onde $d = L(g^{\lambda} \mod n^2)^{-1}$.

DC-Net assimétrica (ADC-Net)

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;

ADC-Net

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;
2. a segurança é baseada em uma função *trapdoor*;

ADC-Net

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;
2. a segurança é baseada em uma função *trapdoor*;
3. usuários podem usar chaves permanentes;

ADC-Net

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;
2. a segurança é baseada em uma função *trapdoor*;
3. usuários podem usar chaves permanentes;
4. processamento tem complexidade máxima polinomial;

ADC-Net

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;
2. a segurança é baseada em uma função *trapdoor*;
3. usuários podem usar chaves permanentes;
4. processamento tem complexidade máxima polinomial;
5. não é necessário uma iteração sobre o número de usuários l, excluindo na consolidação;

ADC-Net

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;
2. a segurança é baseada em uma função *trapdoor*;
3. usuários podem usar chaves permanentes;
4. processamento tem complexidade máxima polinomial;
5. não é necessário uma iteração sobre o número de usuários I, excluindo na consolidação;
6. usuários podem mandar o número mínimo de mensagens;

ADC-Net

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;
2. a segurança é baseada em uma função *trapdoor*;
3. usuários podem usar chaves permanentes;
4. processamento tem complexidade máxima polinomial;
5. não é necessário uma iteração sobre o número de usuários I, excluindo na consolidação;
6. usuários podem mandar o número mínimo de mensagens;
7. usuários podem usar uma função de assinatura para gerar uma assinatura digital $\mathfrak{S}_{i,j}$ de cada uma de suas mensagens $m_{i,j}$;

ADC-Net

[Oli17h]

Satisfaz as seguintes propriedades:

1. o protocolo tem todas as propriedades de uma SDC-Net, excluindo segurança incondicional;
2. a segurança é baseada em uma função *trapdoor*;
3. usuários podem usar chaves permanentes;
4. processamento tem complexidade máxima polinomial;
5. não é necessário uma iteração sobre o número de usuários I, excluindo na consolidação;
6. usuários podem mandar o número mínimo de mensagens;
7. usuários podem usar uma função de assinatura para gerar uma assinatura digital $\mathfrak{S}_{i,j}$ de cada uma de suas mensagens $m_{i,j}$;
8. similar a uma técnica de comprometimento, usuários podem verificar suas mensagens $m_{i,j}$.

ADC-Net

[Oli17h]

Inicialização

Os usuários escolhem um produto de primos n e uma chave privada k_i gerando

$$s = \sum_{i=1}^{I} k_i,$$

de forma que todos saibam do valor de s sem revelar k_i.

ADC-Net

[Oli17h]

Encriptação

$$\text{Enc} : \mathbb{Z}_n \to \mathbb{Z}_{n^2}$$

$$\text{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j + k_i} \mod n^2,$$

ADC-Net

[Oli17h]

Encriptação

$$\begin{aligned} \text{Enc} &: \mathbb{Z}_n \to \mathbb{Z}_{n^2} \\ \text{Enc}_i(m_{i,j}) &\mapsto (1+n)^{m_{i,j}} \cdot g^{h_j + k_i} \mod n^2, \end{aligned}$$

Consolidação

Para gerar a consolidação encriptada $\mathfrak{C}_j$ das mensagens encriptadas $\mathfrak{M}_{i,j}$, os usuários calculam

$$\mathfrak{C}_j = \prod_{i=1}^{I} \mathfrak{M}_{i,j} \mod n^2,$$

ADC-Net

[Oli17h]

Encriptação

$$\mathrm{Enc} : \mathbb{Z}_n \to \mathbb{Z}_{n^2}$$

$$\mathrm{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j + k_i} \mod n^2,$$

Descriptografar

$$\mathrm{Dec} : \mathbb{Z}_{n^2} \to \mathbb{Z}_n$$

$$\mathrm{Dec}\left(\mathfrak{C}_j\right) \mapsto \frac{\left(\mathfrak{C}_j \cdot g^{-l \cdot h_j - s} \mod n^2\right) - 1}{n},$$

onde $s = \sum_{i=1}^{l} k_i$.

ADC-Net

Notas

1. Podemos construir várias ADC-Nets.

ADC-Net

Notas

1. Podemos construir várias ADC-Nets.
2. A verificação é semelhante a técnicas de compromisso.

ADC-Net

Notas

1. Podemos construir várias ADC-Nets.
2. A verificação é semelhante a técnicas de compromisso.
3. Para vários tipos de verificação seria melhor usar $g^{h_j \times k_i}$ em vez de $g^{h_j + k_i}$.

ADC-Net

Notas

1. Podemos construir várias ADC-Nets.
2. A verificação é semelhante a técnicas de compromisso.
3. Para vários tipos de verificação seria melhor usar $g^{h_j \times k_i}$ em vez de $g^{h_j + k_i}$.
4. Devemos usar assinatura digital.

Verificação

$$\mathfrak{U}_i = \prod_{j=1}^{J} \mathfrak{M}_{i,j}$$

e

$$\mathfrak{H} = \prod_{j=1}^{J} g^{h_j}$$

O usuário i calcula

$$\mathfrak{V}_i = \prod_{j=1}^{J} (1+n)^{m_{i,j}} \cdot g^{k_i} \mod n^2.$$

A função de abertura Open pode determina se os valores estão corretos

$$\text{Open}\left(\mathfrak{U}_i, \mathfrak{V}_i, \mathfrak{H}\right) = \left(\mathfrak{U}_i \stackrel{?}{=} \mathfrak{V}_i \cdot \mathfrak{H}\right).$$

Usuário Adversário

Detectando a mensagem $m_{i,j}$ com um valor gigante.

	1	2	$\cdots$	j	$\cdots$	J	b_i
1	$m_{1,1}$	$m_{1,2}$	$\cdots$	$m_{1,j}$	$\cdots$	$m_{1,J}$	$\sum_{j=1}^{J} m_{1,j}$
2	$m_{2,1}$	$m_{2,2}$	$\cdots$	$m_{2,j}$	$\cdots$	$m_{2,J}$	$\sum_{j=1}^{J} m_{2,j}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
i	$m_{i,1}$	$m_{i,2}$	$\cdots$	$m_{i,j}$	$\cdots$	$m_{i,J}$	$\sum_{j=1}^{J} m_{i,j}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
I	$m_{I,1}$	$m_{I,2}$	$\cdots$	$m_{I,j}$	$\cdots$	$m_{I,J}$	$\sum_{j=1}^{J} m_{I,j}$
c_j	$\sum_{i=1}^{I} m_{i,1}$	$\sum_{i=1}^{I} m_{i,2}$	$\cdots$	$\sum_{i=1}^{I} m_{i,j}$	$\cdots$	$\sum_{i=1}^{I} m_{i,J}$	$\sum_{j=1}^{j} c_j = \sum_{i=1}^{I} b_i$

Detectando Antes

$\mathcal{U}_1 \cup \mathcal{U}_1 = \mathcal{U}.$

$$\text{Usuários :} \qquad v = \sum_{i \in \mathcal{U}_1} m_{i,j} \qquad \text{e} \qquad \mathfrak{V} = \prod_{i \in \mathcal{U}_1} g^{h_j + k_i} \mod n^2.$$

$$\text{Contador :} \qquad \mathfrak{P} = \prod_{i \in \mathcal{U}_1} \mathfrak{M}_{i,j}$$

$$\text{Open}\left(\mathfrak{P}, \mathfrak{V}, v\right) = \left(\mathfrak{P} \stackrel{?}{=} (1+n)^v \cdot \mathfrak{V} \mod n^2\right).$$

Suponha que o problema está no $\mathcal{U}_1$, logo podemos separar os usuários do conjunto $\mathcal{U}_1$ em dois conjuntos $\mathcal{U}_{1_1}$ e $\mathcal{U}_{1_2}$, tal que

$$\mathcal{U}_{1_1} \cup \mathcal{U}_{1_2} = \mathcal{U}_1.$$

Para não comprometermos a privacidade:

$$\mathcal{U}_{1_1} \cup \mathcal{U}_{1_2} = \mathcal{U}_1 \cup \mathcal{U}_2.$$

O processo recursivo leva a detecção do usuário em $\log_2(I)$ passos.

Tópicos

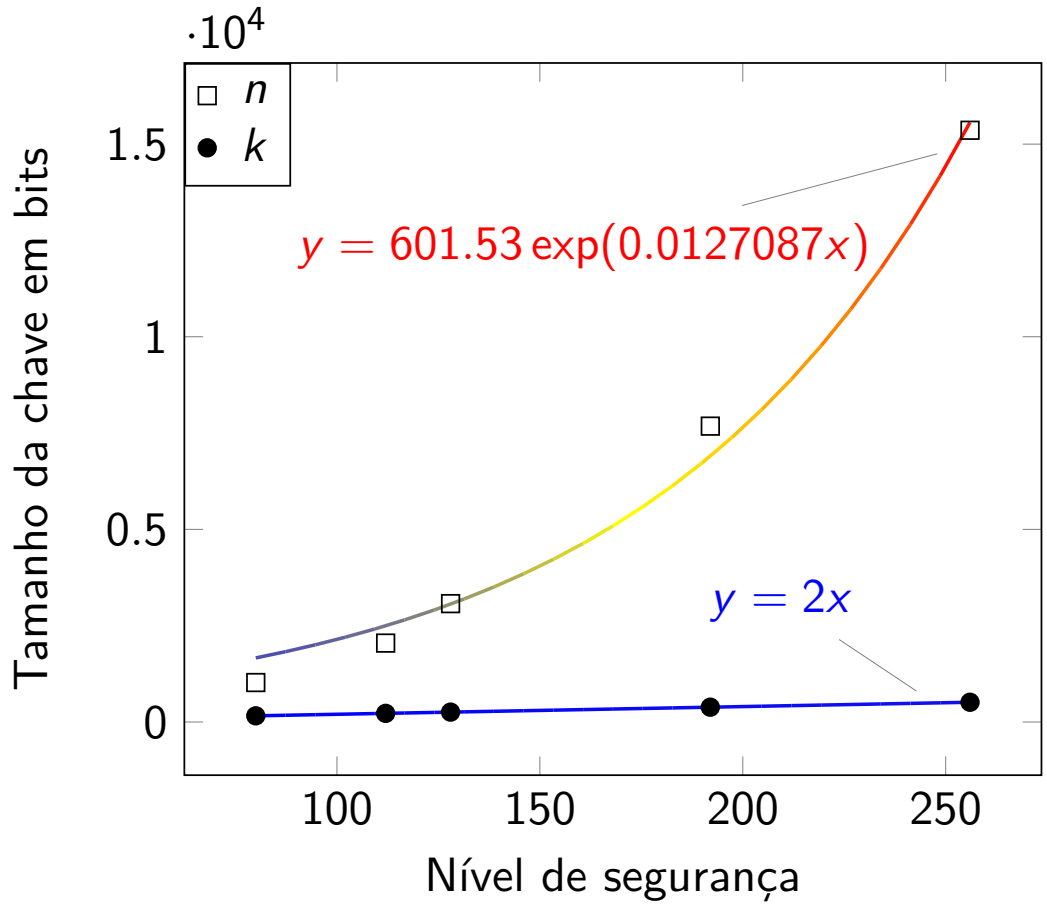
Complexidade computacional

Técnica	Enc	Consolidação	Dec
SDC-Net	$O(I)$	NA	$O(I)$
Compromisso	$O(\log(k))$	$O(J)$ ou $O(I)$	$O(k)$
PCHA	$O(\log(n))$	$O(I)$	$O(\log(n))$
ADC-Net	$O(\log(k))$	$O(I)$	$O(\log(k))$

Crescimento de k e n

[Oli17b]

Nível	k	n
80	160	1 024
112	224	2 048
128	256	3 072
192	384	7 680
256	512	15 360

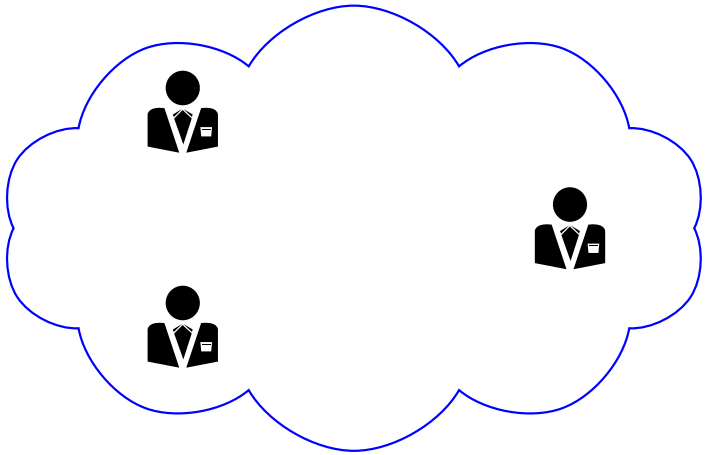


Comparação das propriedades

Propriedades	**SDC-Net**	**PCHA**	**ADC-Net**
Evita conluio	✓		✓
Conjunto de usuários confiáveis	✓		✓
Mensagens direto para o destinatário	✓		✓
Usuários podem descriptografar	✓		✓
Número mínimo de mensagens	✓	✓	✓
Escalável		✓	✓
Chaves permanentes	✓	✓	✓
Baseado em *trapdoors*	✓	✓	✓
Chaves armazenadas por usuário	$2(l-1)$	1	1
Total de chaves	$O(l^2)$	2	$O(l)$
Tempo polinomial	✓	✓	✓
Possibilidade de verificação			✓
Não se pode romper o protocolo			✓

PPP1 - SDC-Nets

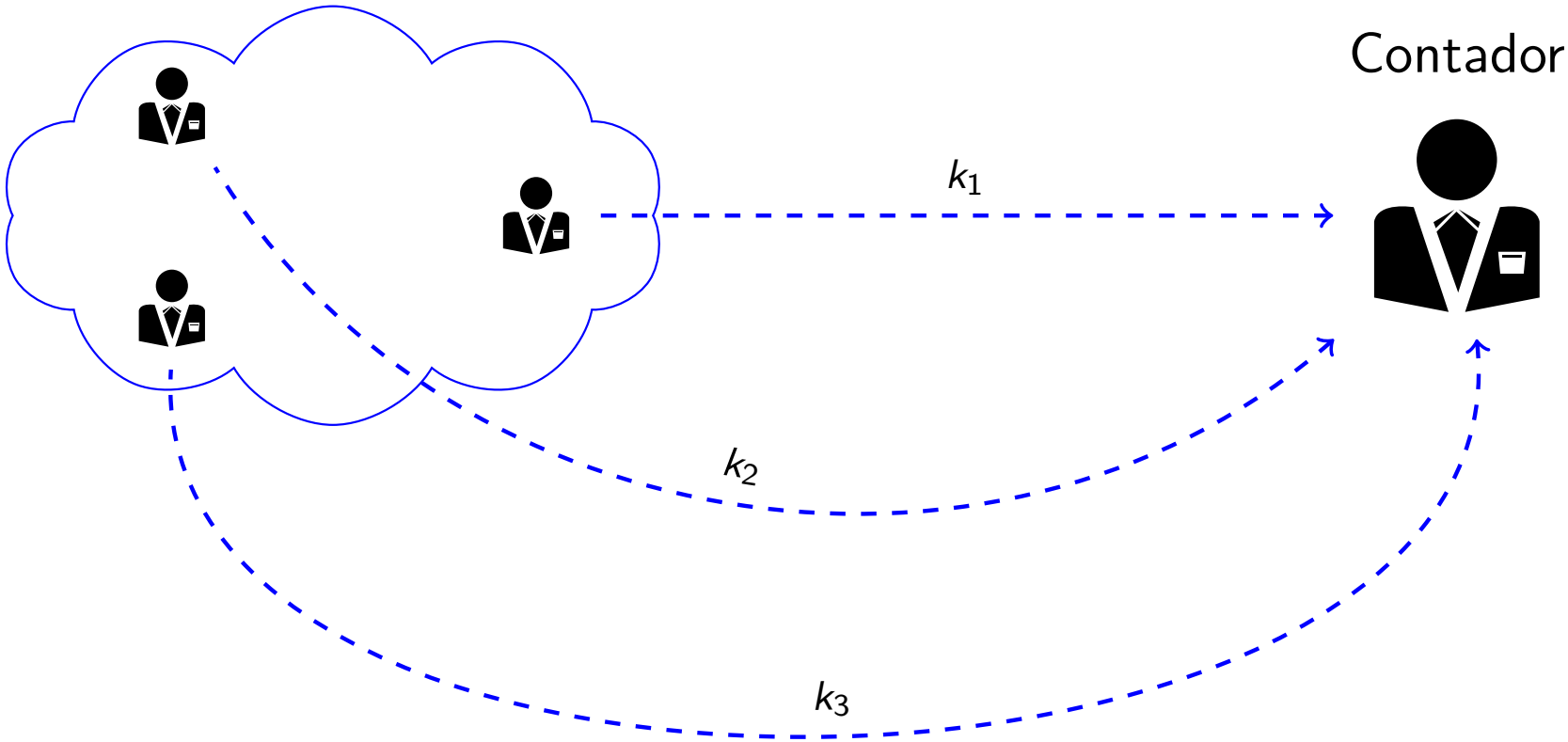
SDC-Nets Usando In-Network Aggregation [BM14]



Contador

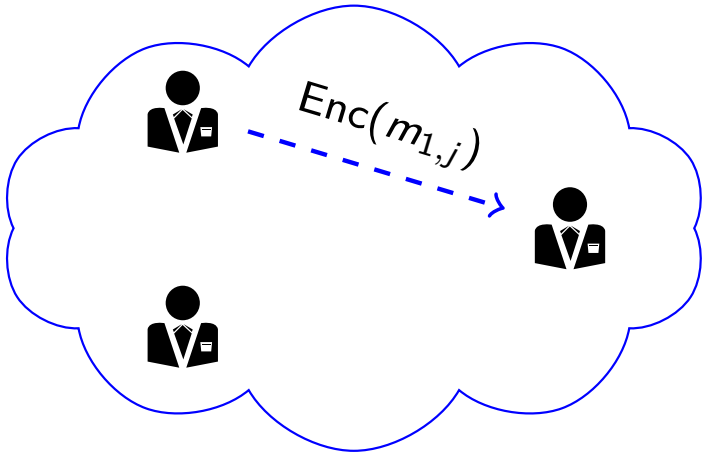
PPP1 - SDC-Nets

SDC-Nets Usando In-Network Aggregation [BM14]



PPP1 - SDC-Nets

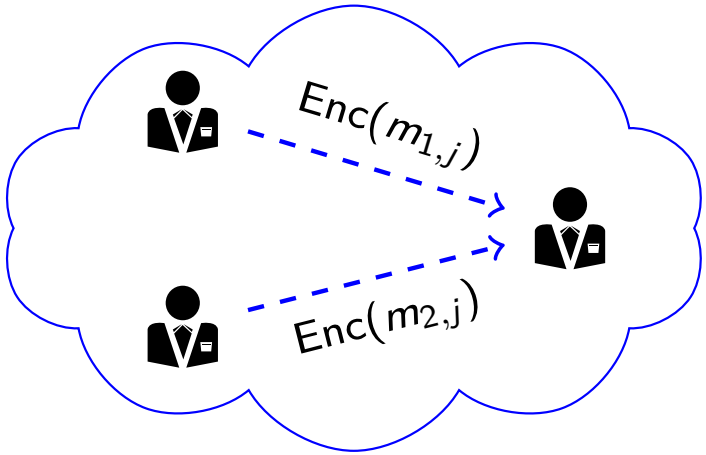
SDC-Nets Usando In-Network Aggregation [BM14]



Contador

PPP1 - SDC-Nets

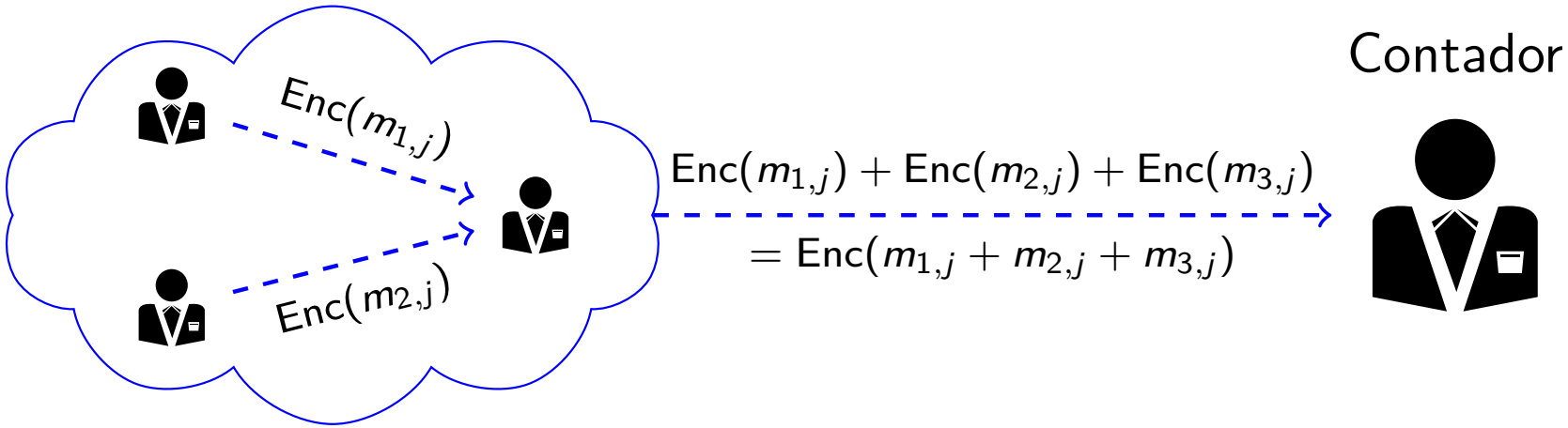
SDC-Nets Usando In-Network Aggregation [BM14]



Contador

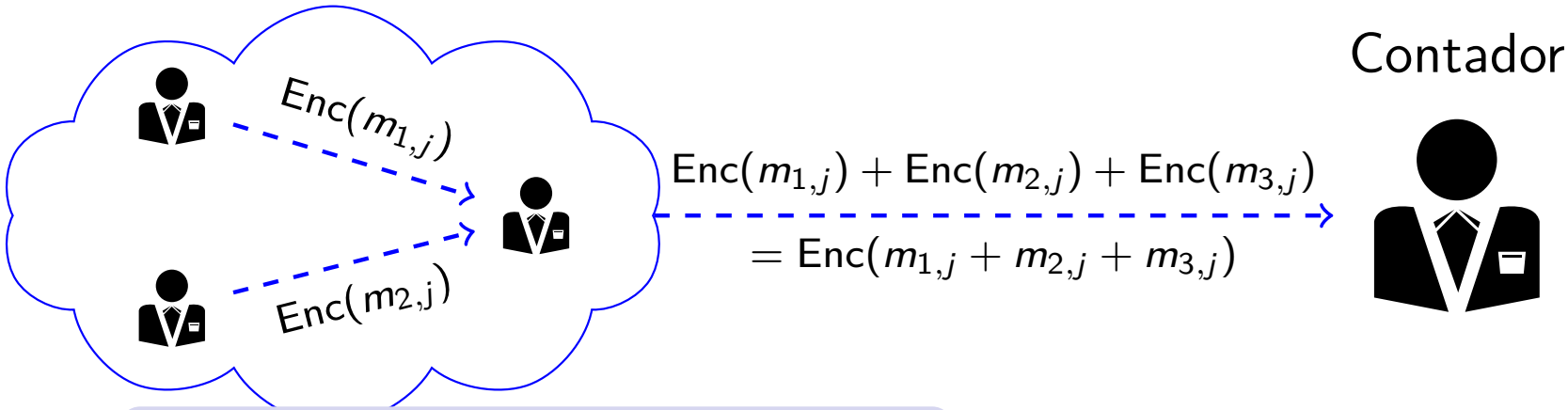
PPP1 - SDC-Nets

SDC-Nets Usando In-Network Aggregation [BM14]



PPP1 - SDC-Nets

SDC-Nets Usando In-Network Aggregation [BM14]

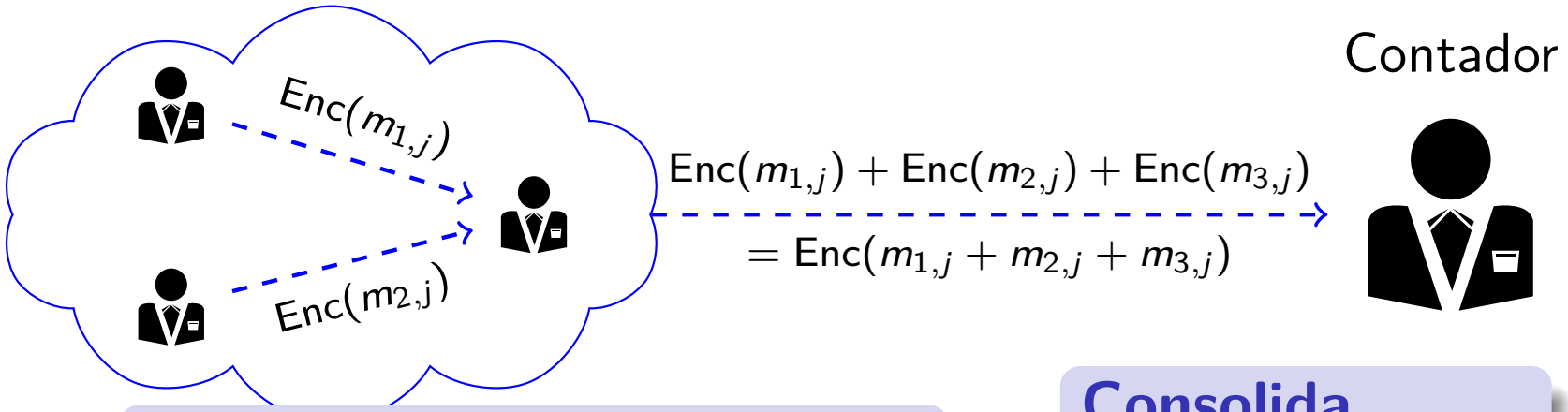


Cifra

$$\mathfrak{M}_{i,j} = \mathsf{Enc}(m_{i,j}) = m_{i,j} + \mathsf{H}(k_i||j)$$

PPP1 - SDC-Nets

SDC-Nets Usando In-Network Aggregation [BM14]



Cifra

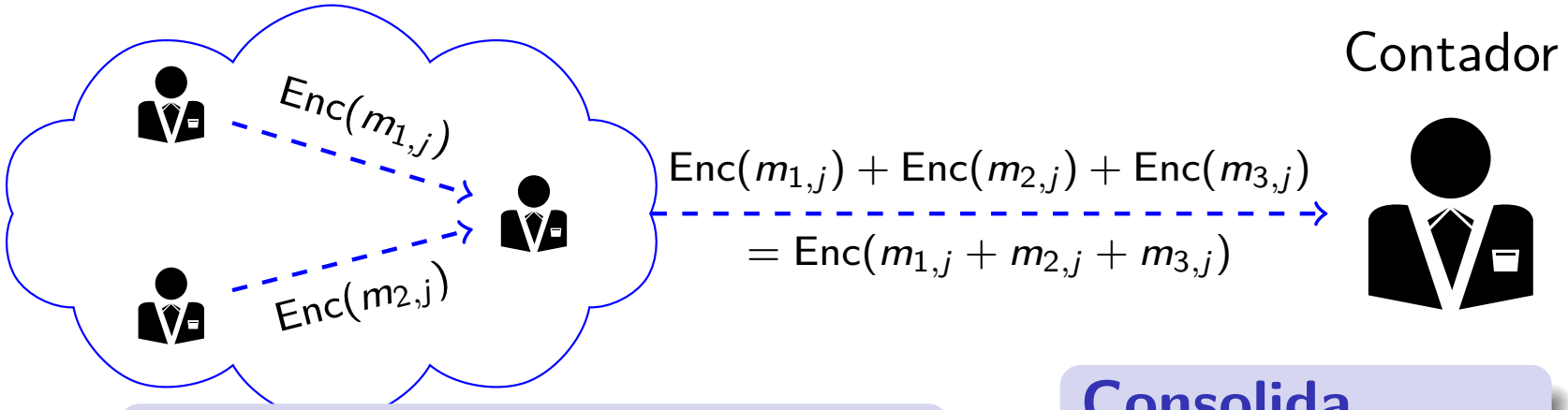
$$\mathfrak{M}_{i,j} = \mathsf{Enc}(m_{i,j}) = m_{i,j} + \mathsf{H}(k_i||j)$$

Consolida

$$\mathfrak{C}_j = \sum_{i=1}^{N} \mathfrak{M}_{i,j}$$

PPP1 - SDC-Nets

SDC-Nets Usando In-Network Aggregation [BM14]



Cifra

$$\mathfrak{M}_{i,j} = \mathsf{Enc}(m_{i,j}) = m_{i,j} + \mathsf{H}(k_i||j)$$

Consolida

$$\mathfrak{C}_j = \sum_{i=1}^{N} \mathfrak{M}_{i,j}$$

Descifra

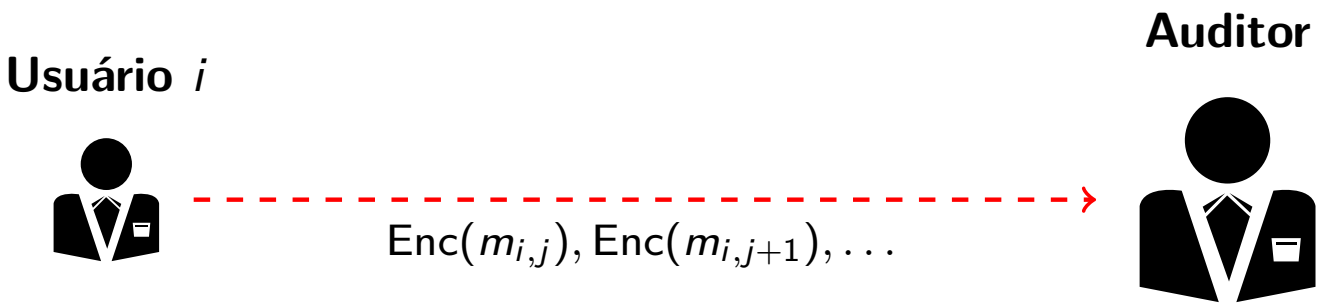
$$\mathsf{Dec}\left(\mathfrak{C}_j\right) = \mathfrak{C}_j - \sum_{i=1}^{N} \mathsf{H}(k_i||j) = \sum_{i=1}^{N} m_{i,j}$$

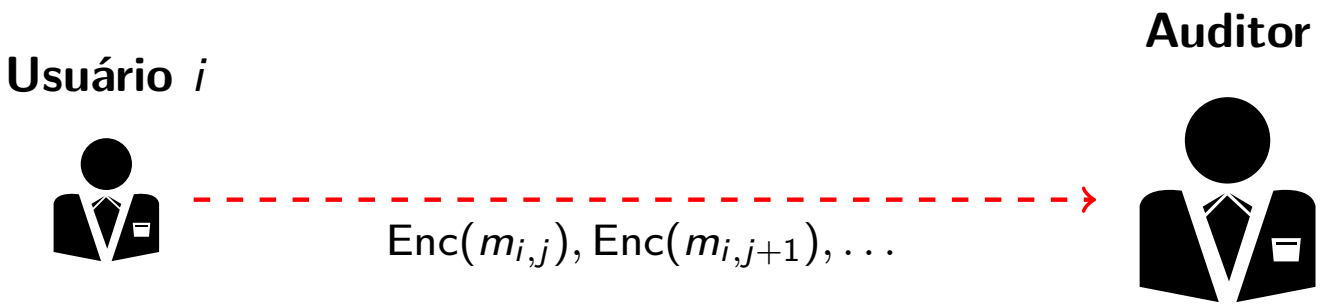
Usuário *i*

Auditor

PPP2

Curvas Elípticas

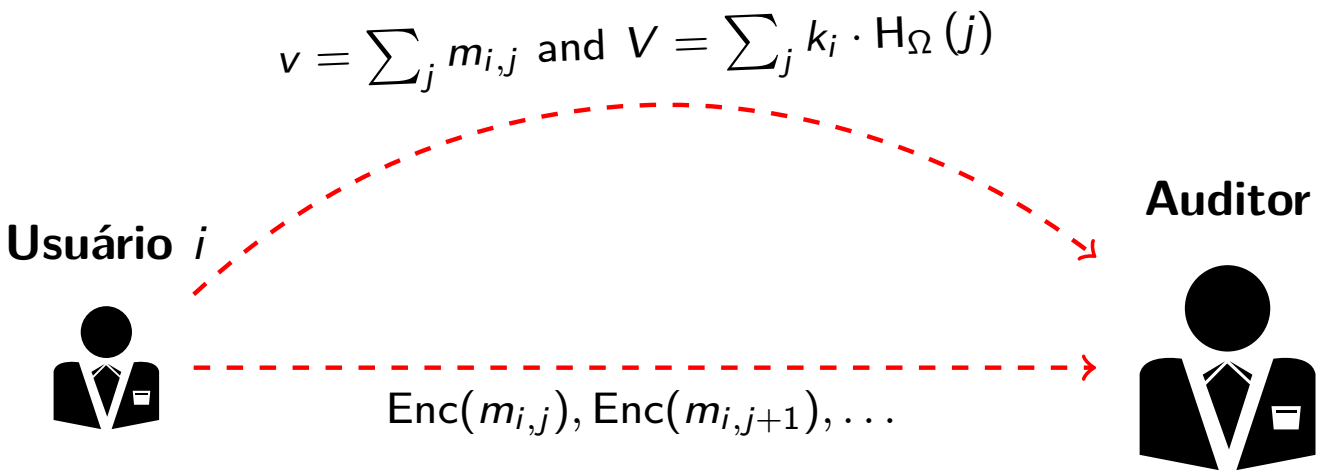




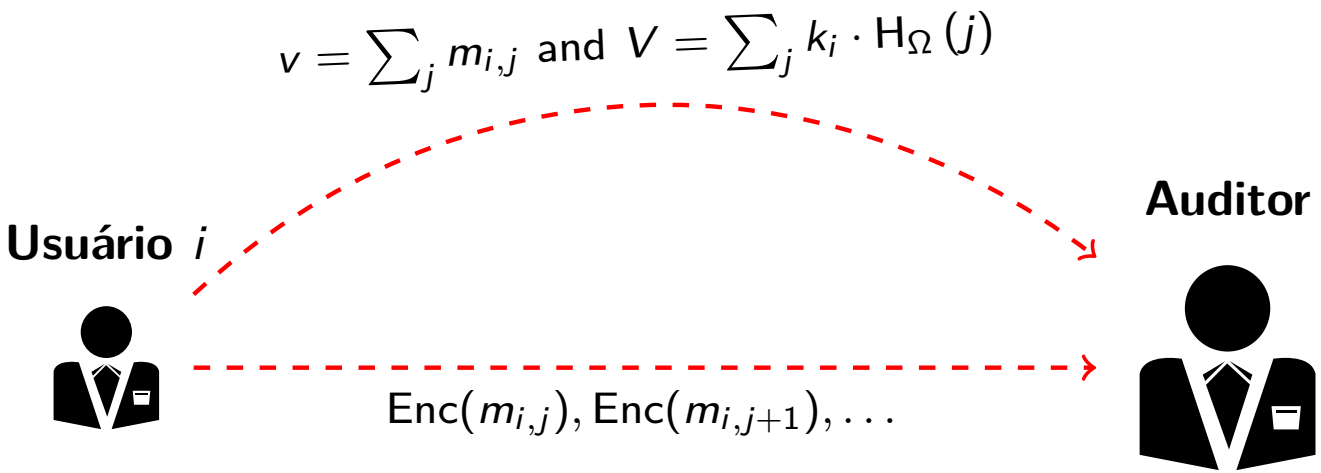
$$Q = \sum_j \mathrm{Enc}(m_{i,j}) = \sum_j k_i \cdot \mathrm{H}_\Omega(j) + m_{i,j} \cdot P$$

PPP2

Curvas Elípticas



$$Q = \sum_j \mathrm{Enc}(m_{i,j}) = \sum_j k_i \cdot \mathrm{H}_\Omega(j) + m_{i,j} \cdot P$$

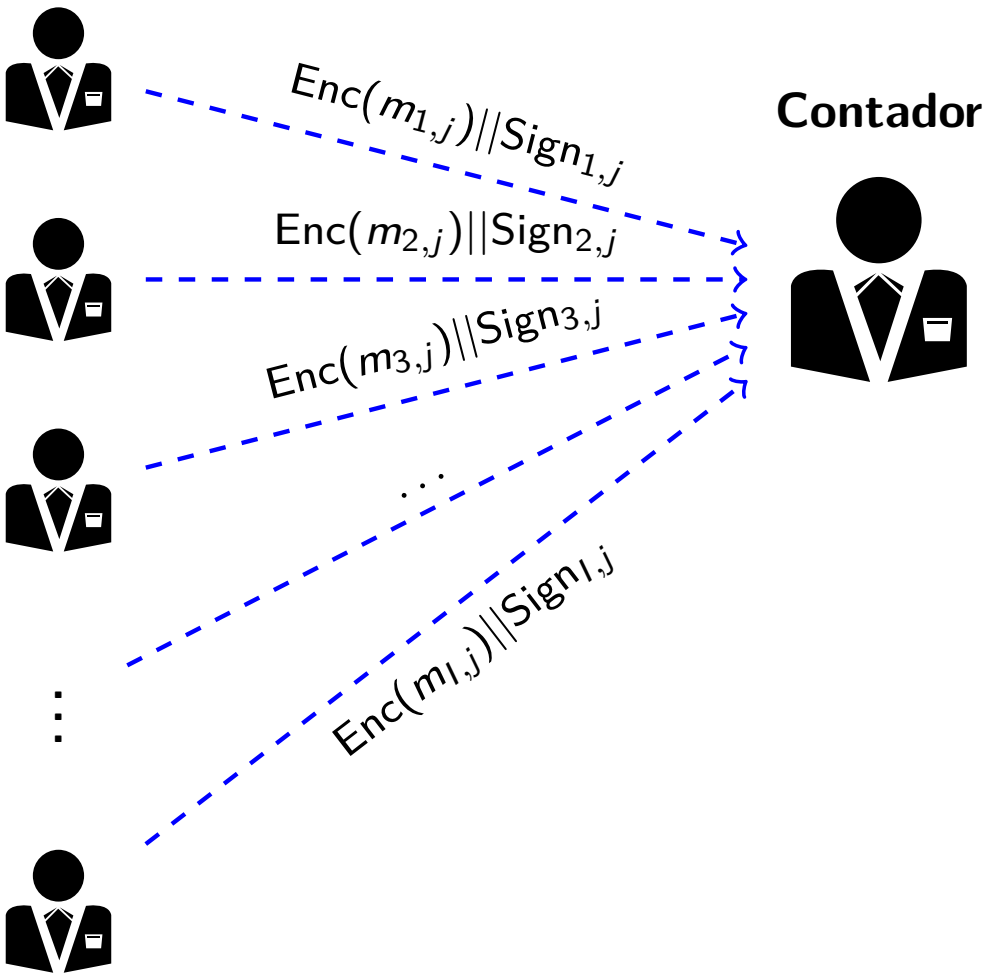


$$Q = \sum_j \mathrm{Enc}(m_{i,j}) = \sum_j k_i \cdot \mathrm{H}_\Omega(j) + m_{i,j} \cdot P$$

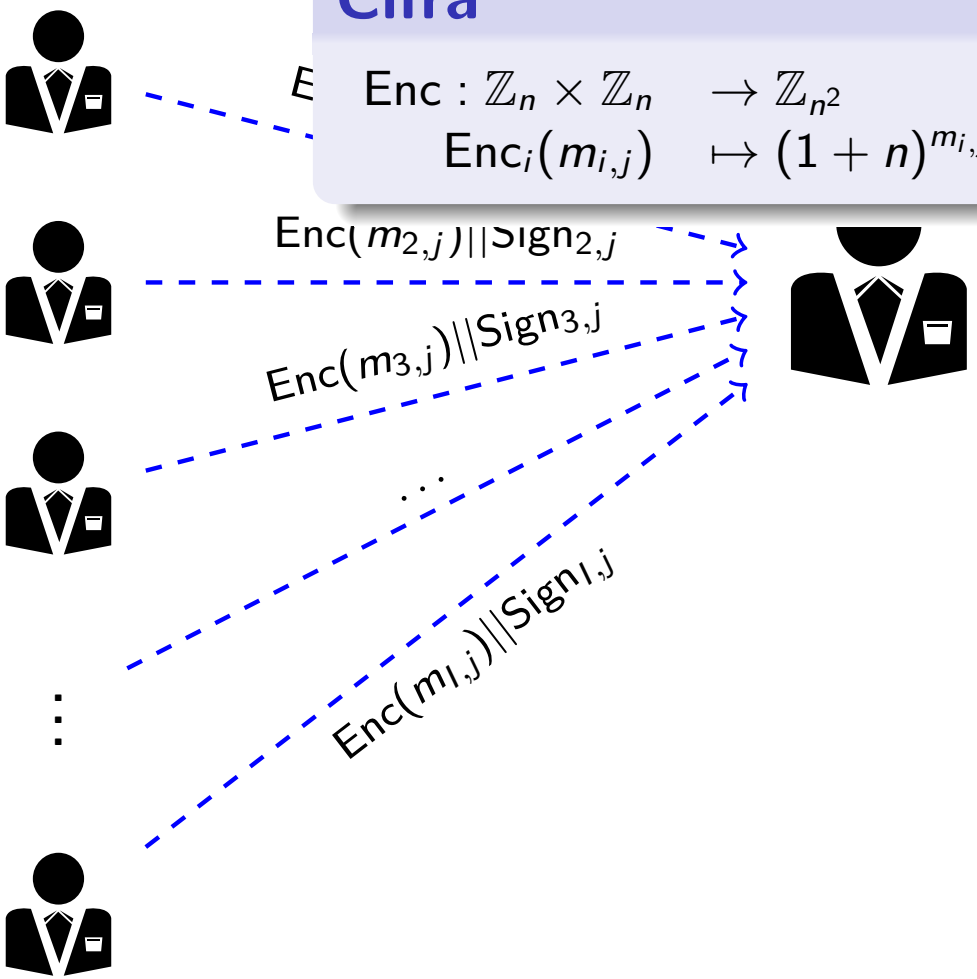
Verification

$$v \cdot P \stackrel{?}{=} Q - V$$

Usuários

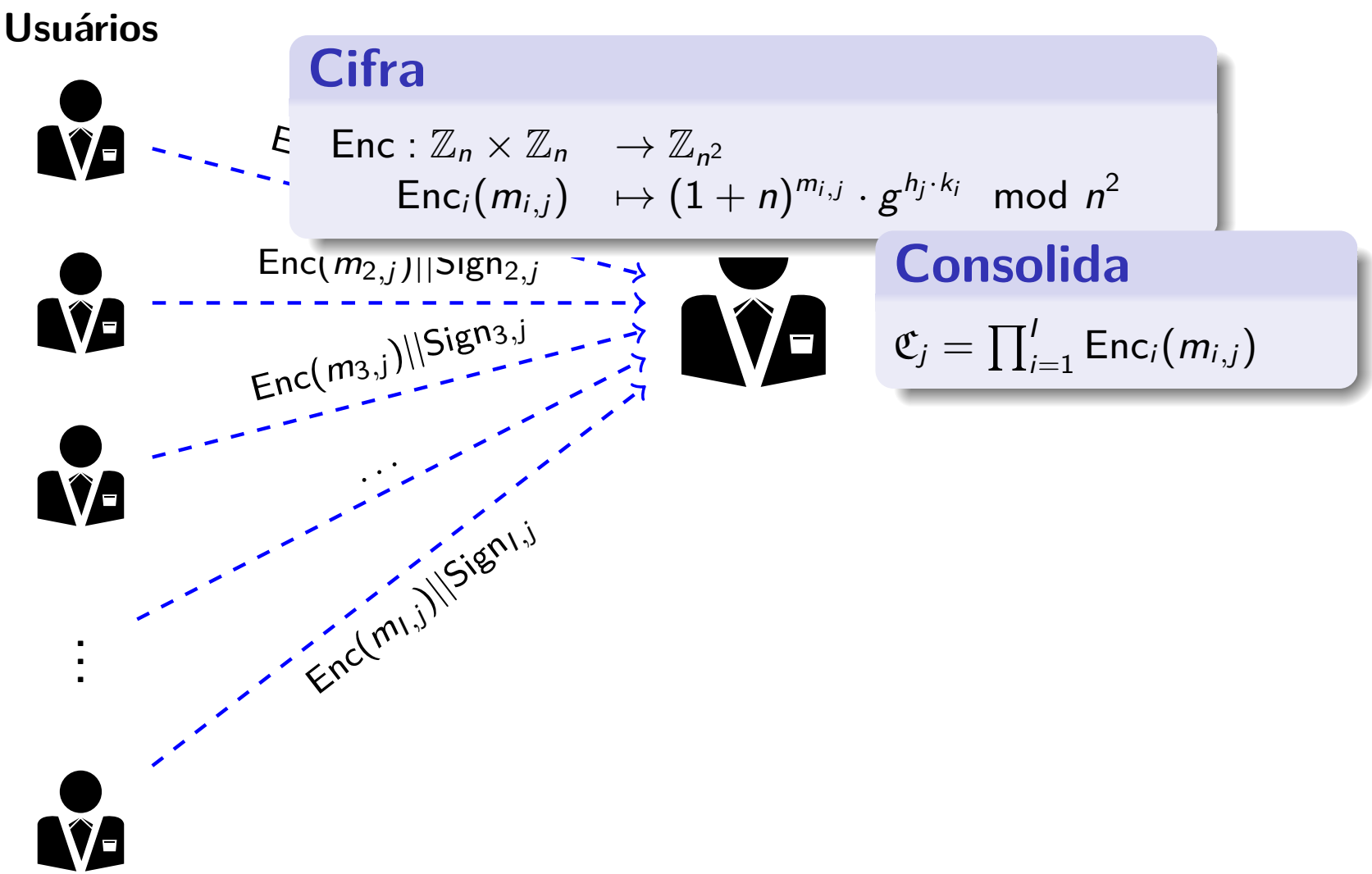

Contador
$Enc(m_{1,j})||Sign_{1,j}$
$Enc(m_{2,j})||Sign_{2,j}$
$Enc(m_{3,j})||Sign_{3,j}$
...
$Enc(m_{l,j})||Sign_{l,j}$

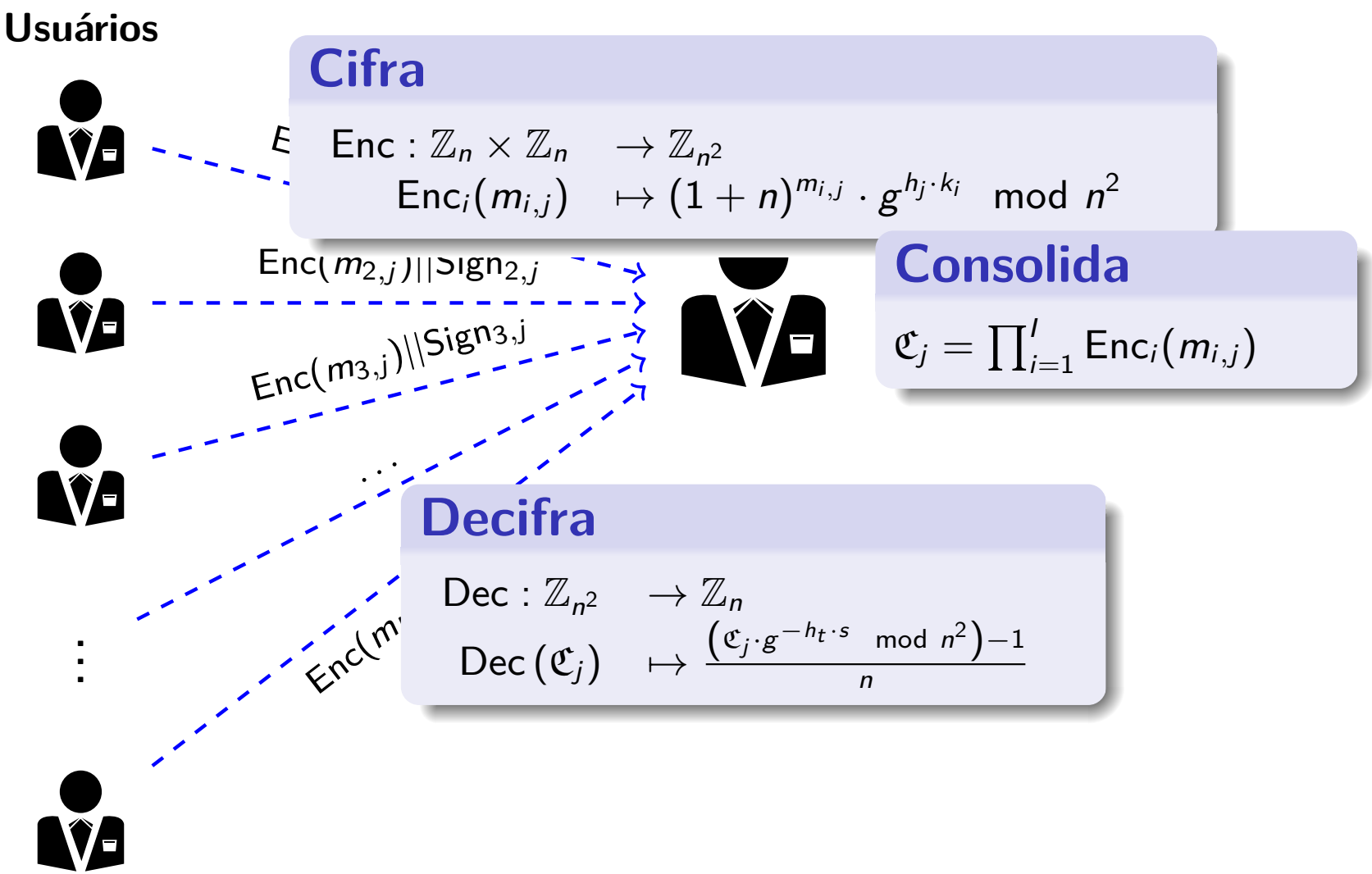
Usuários

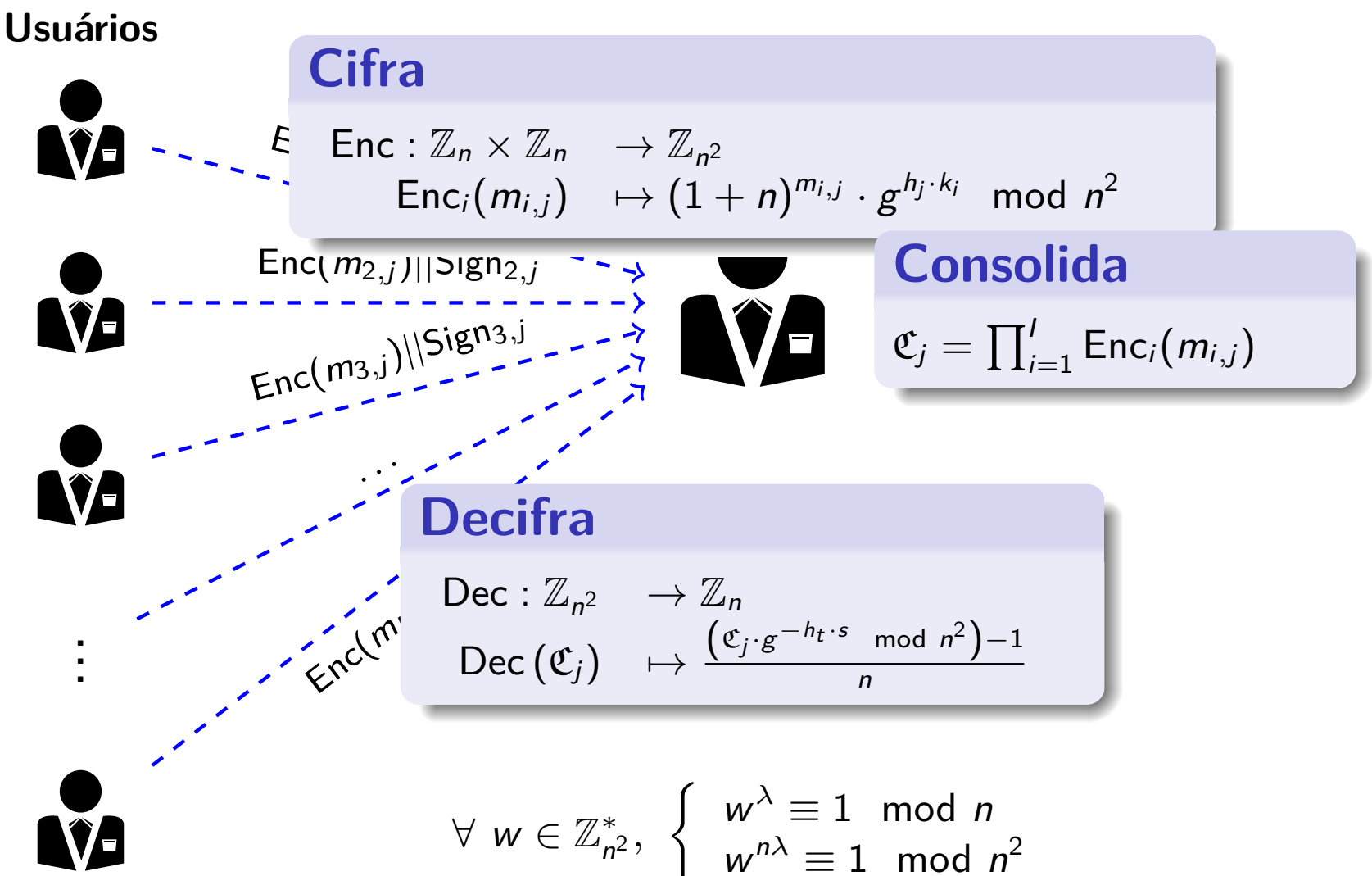


Cifra

$$\begin{aligned} \text{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z}_{n^2} \\ \text{Enc}_i(m_{i,j}) &\mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \mod n^2 \end{aligned}$$

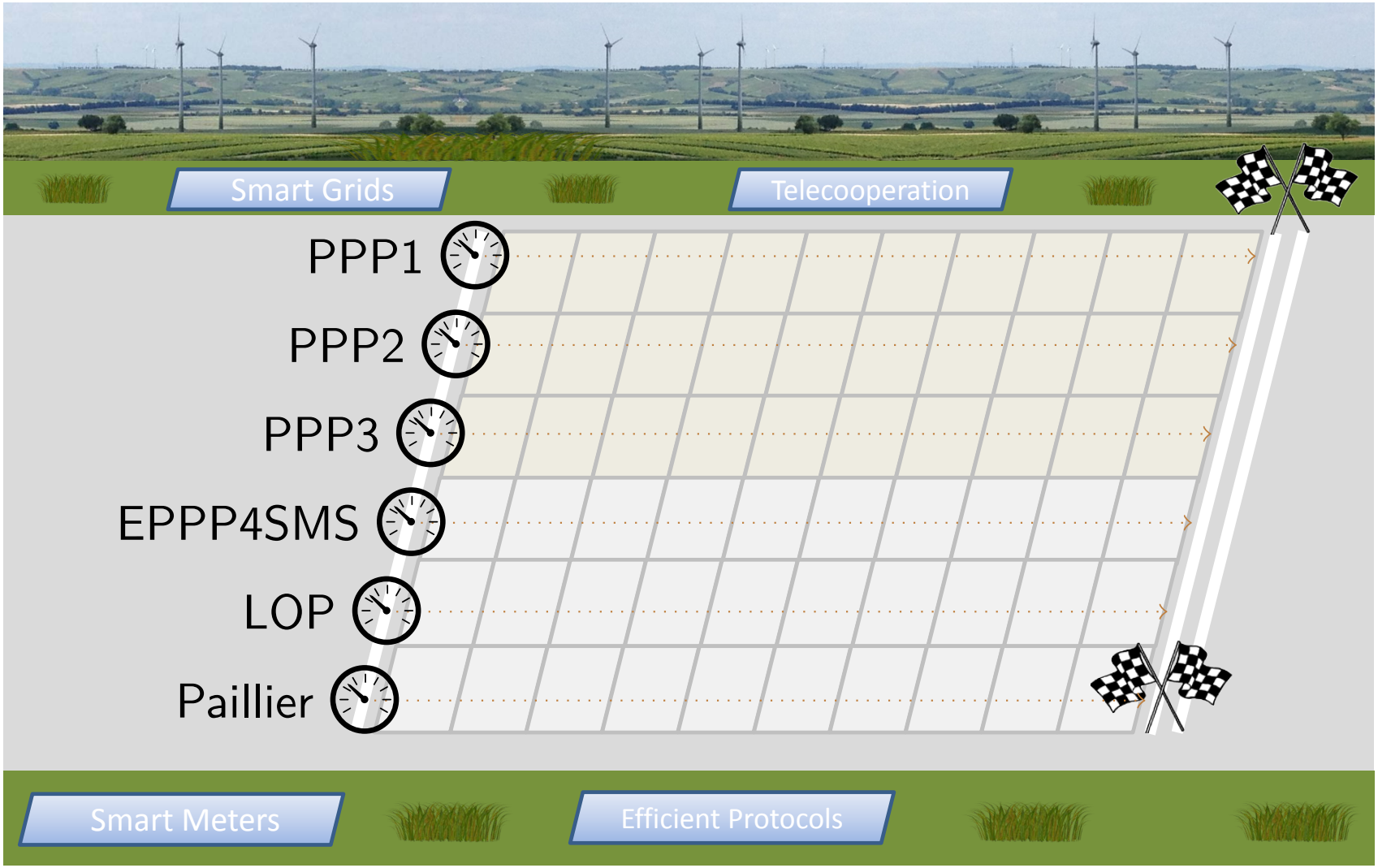

Usuários
Cifra
$\mathrm{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_{n^2}$
$\mathrm{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \mod n^2$
Consolida
$\mathfrak{C}_j = \prod_{i=1}^{I} \mathrm{Enc}_i(m_{i,j})$
$\mathrm{Enc}(m_{2,j})||\mathrm{Sign}_{2,j}$
$\mathrm{Enc}(m_{3,j})||\mathrm{Sign}_{3,j}$
...
$\mathrm{Enc}(m_{I,j})||\mathrm{Sign}_{I,j}$


Usuários
Cifra
$\text{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{n^2}$
$\text{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \mod n^2$
$\text{Enc}(m_{2,j})||\text{Sign}_{2,j}$
$\text{Enc}(m_{3,j})||\text{Sign}_{3,j}$
Consolida
$\mathfrak{C}_j = \prod_{i=1}^{I} \text{Enc}_i(m_{i,j})$
Decifra
$\text{Dec} : \mathbb{Z}_{n^2} \rightarrow \mathbb{Z}_n$
$\text{Dec}(\mathfrak{C}_j) \mapsto \frac{(\mathfrak{C}_j \cdot g^{-h_t \cdot s} \mod n^2) - 1}{n}$


Usuários
Cifra
$\text{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_{n^2}$
$\text{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \mod n^2$
Consolida
$\mathfrak{C}_j = \prod_{i=1}^{I} \text{Enc}_i(m_{i,j})$
$\text{Enc}(m_{2,j})||\text{Sign}_{2,j}$
$\text{Enc}(m_{3,j})||\text{Sign}_{3,j}$
Decifra
$\text{Dec} : \mathbb{Z}_{n^2} \to \mathbb{Z}_n$
$\text{Dec}(\mathfrak{C}_j) \mapsto \frac{(\mathfrak{C}_j \cdot g^{-h_t \cdot s} \mod n^2) - 1}{n}$
$\forall\ w \in \mathbb{Z}^*_{n^2}, \begin{cases} w^{\lambda} \equiv 1 \mod n \\ w^{n\lambda} \equiv 1 \mod n^2 \end{cases}$

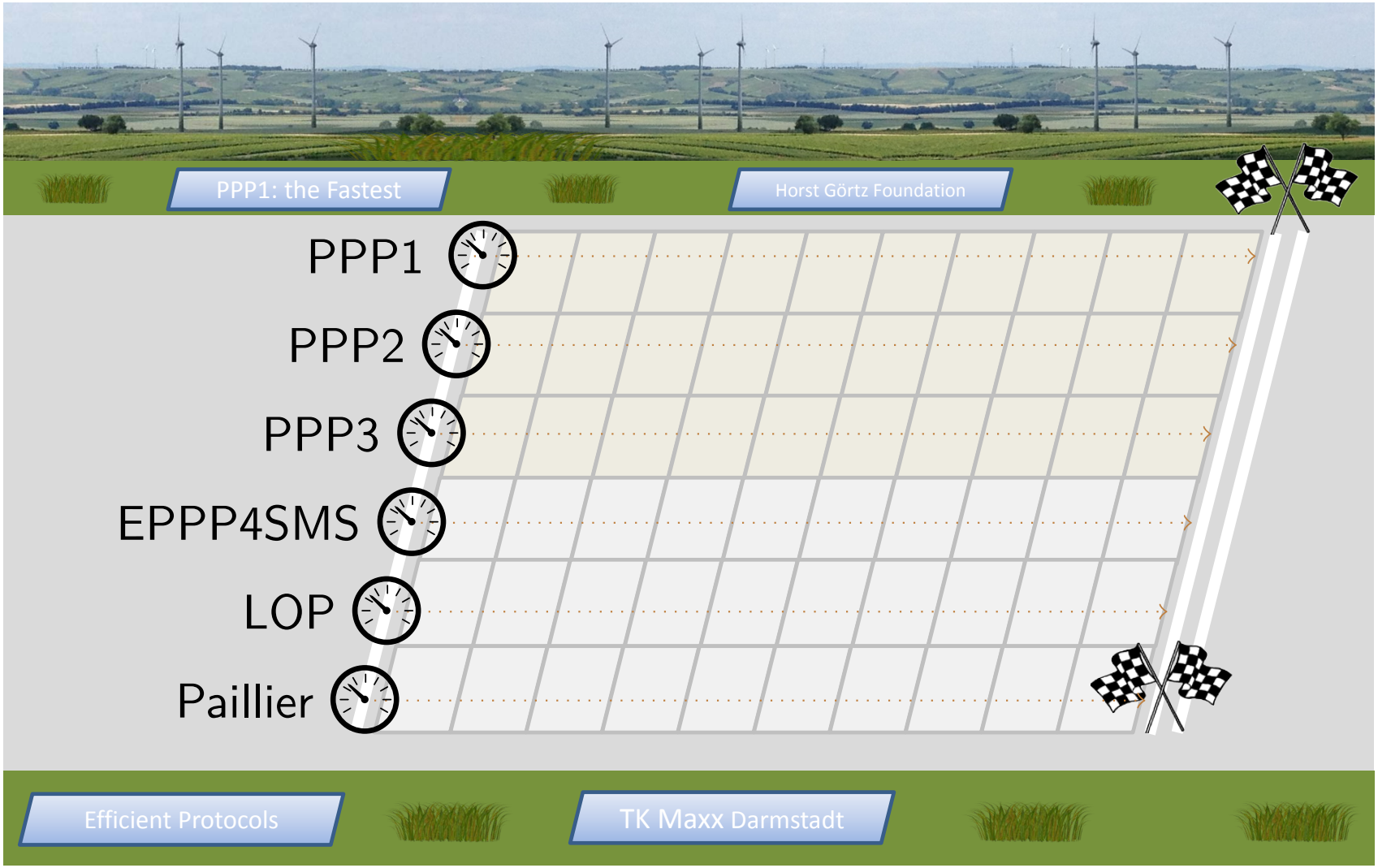
Performance

Corrida de protocolos [Oli17i]



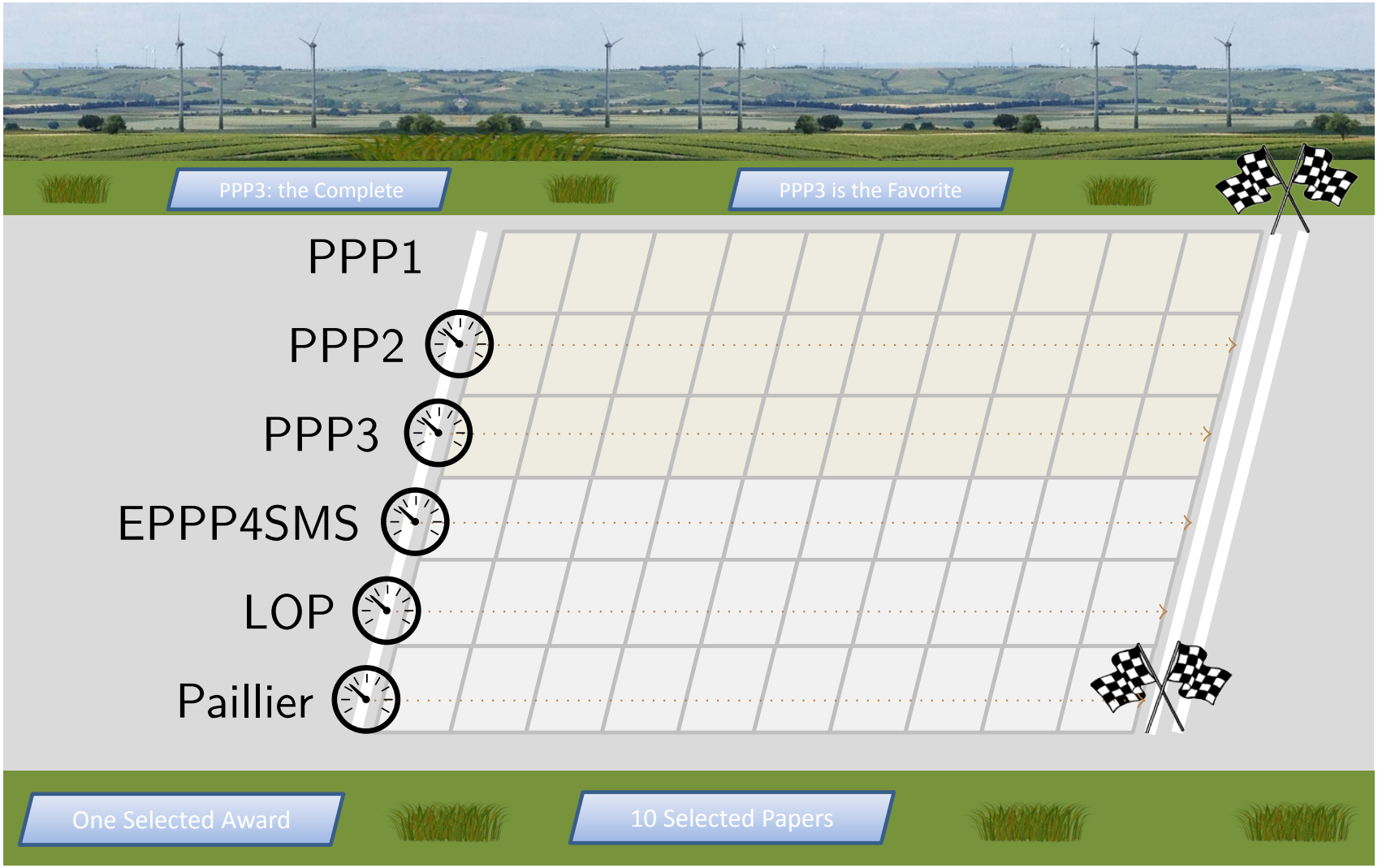
Performance

Corrida de protocolos



Performance

Corrida de protocolos

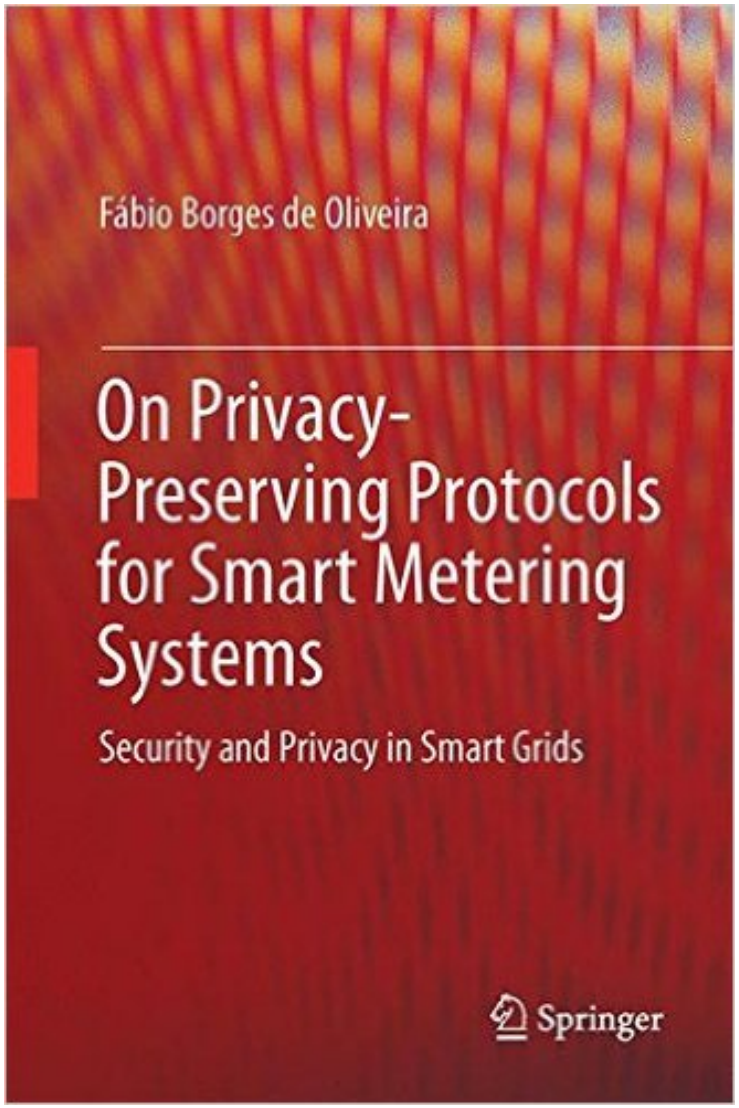


Tópicos

Conclusões

[Oli17d]

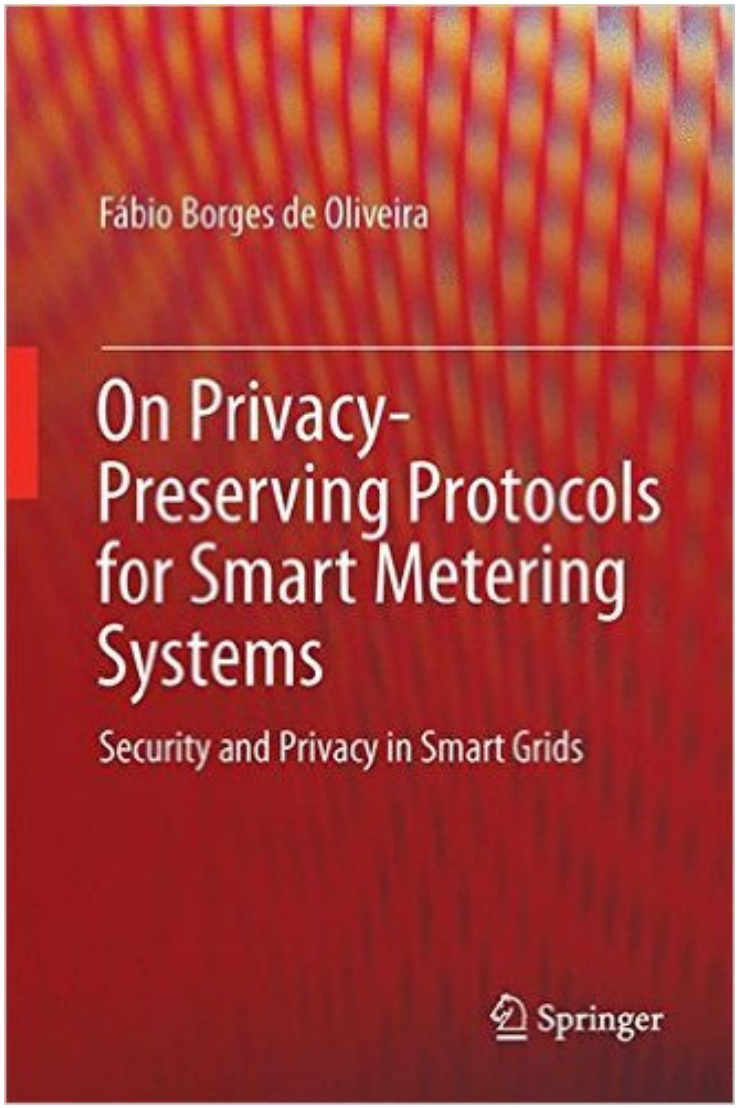
- Segurança



Conclusões

[Oli17d]

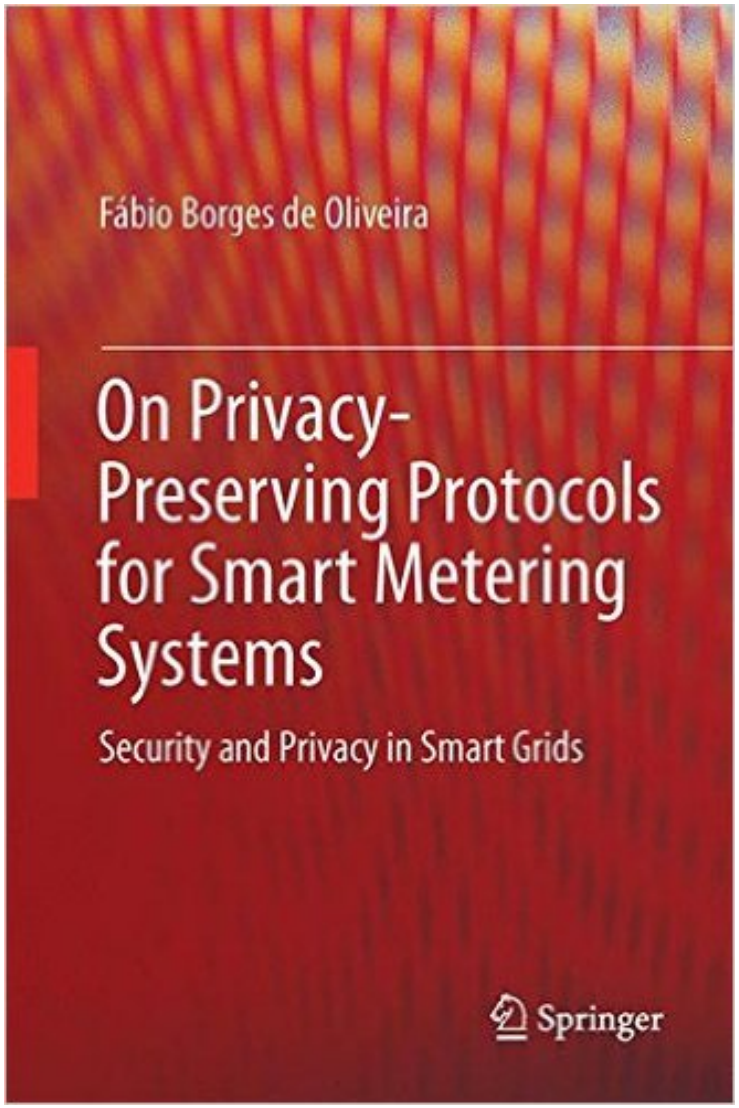
- Segurança
- Privacidade



Conclusões

[Oli17d]

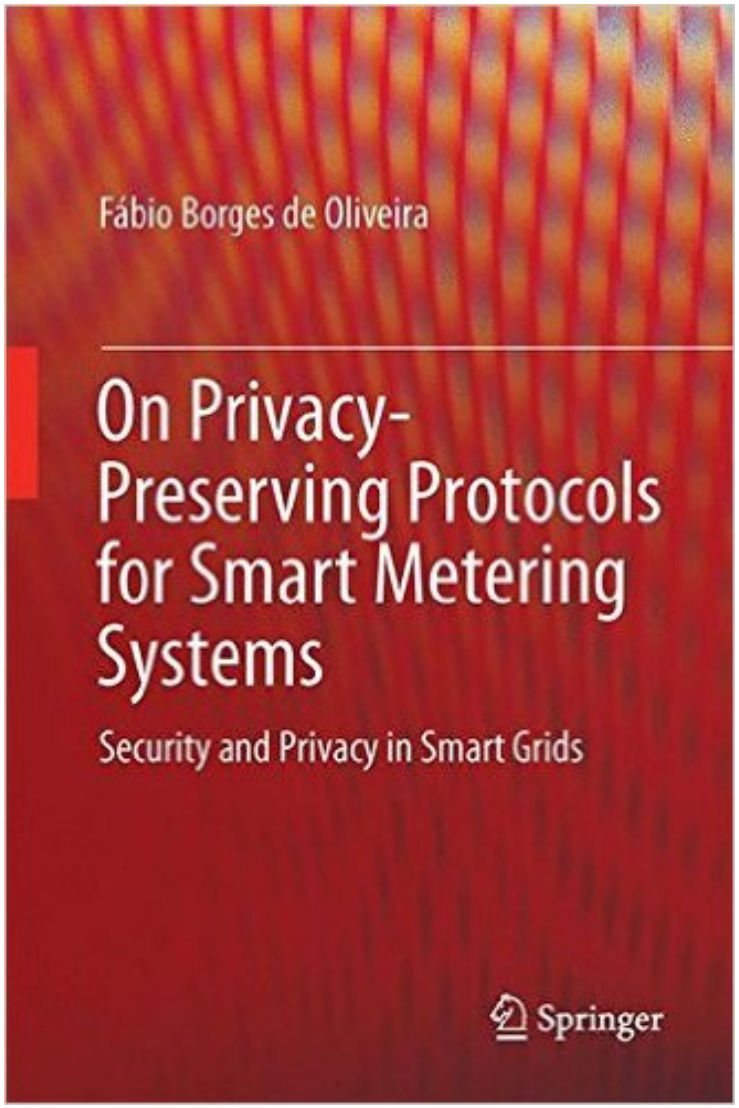
- Segurança
- Privacidade
- Verificação



Conclusões

[Oli17d]

- Segurança
- Privacidade
- Verificação
- ADC-Net



Thank You!

All comments and suggestions are welcomed.

Contact: borges@lncc.br

Bibliography I

Fábio Borges e Leonardo A. Martucci. Ikup keeps users' privacy in the smart grid. Em *IEEE conference on communications and network security, CNS 2014, san francisco, ca, usa, october 29-31, 2014*, 2014, páginas 310–318.

Fábio Borges. *Privacy-preserving data aggregation in smart metering systems*. Em. *Smarter energy: from smart metering to the smart grid*. H. Sun, N. Hatziargyriou, L. Carpanini e H.V. Poor, editores. Em Energy Engineering Series. Institution of Engineering & Technology, 2016.

Ronald Cramer, Rosario Gennaro e Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. Em *Proceedings of the 16th annual international conference on theory and application of cryptographic techniques*. Em EUROCRYPT'97. Springer-Verlag, Konstanz, Germany, 1997, páginas 103–118.

David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. acm*, 24(2):84–90, fevereiro de 1981.

Bibliography II

D. Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability. *J. cryptol.*, 1(1):65–75, março de 1988.

Dimitris A Gritzalis. Principles and requirements for a secure e-voting system. *Computers & security*, 21(6):539 –556, 2002.

Fábio Borges de Oliveira. *A selective review*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 25–36.

Fábio Borges de Oliveira. *Analytical comparison*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 101–110.

Fábio Borges de Oliveira. *Background and models*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 13–23.

Bibliography III

Fábio Borges de Oliveira. *Concluding remarks*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 127–129.

Fábio Borges de Oliveira. *Introduction*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 3–12.

Fábio Borges de Oliveira. *Quantifying the aggregation size*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 49–60.

Fábio Borges de Oliveira. *Reasons to measure frequently and their requirements*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 39–47.

Bibliography IV

Fábio Borges de Oliveira. *Selected privacy-preserving protocols*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 61–100.

Fábio Borges de Oliveira. *Simulation and validation*. Em. *On privacy-preserving protocols for smart metering systems: security and privacy in smart grids*. Springer International Publishing, Cham, 2017, páginas 111–126.

Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. Em, *Advances in cryptology - eurocrypt 1999*. Volume 1592, em Lecture Notes in Computer Science, páginas 223–238. Springer, 1999.

Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. Em *Proceedings of the 11th annual international cryptology conference on advances in cryptology*. Em CRYPTO '91. Springer-Verlag, London, UK, UK, 1992, páginas 129–140.