O Computador para o Século 21: Desafios de Segurança e Privacidade após 25 Anos

SBSeg 2017

Leonardo Oliveira UFMG Fernando Pereira UFMG

Rafael Misoczki intel Diego Aranha UNICAMP

Fábio Borges

Michele Nogueira UFPR Michelle Wangham UNIVALI

Roteiro

Introdução

Em 1991, Mark Weiser descreveu uma visão do *computador para o século 21* [Wei91]

Introdução

Em 1991, Mark Weiser descreveu uma visão do *computador para o século 21* [Wei91]

- Ubiquitous Computing (UbiComp) [Wei93; LY02]
  - Wireless Sensor Networks [EGH+99; PK00]
  - Internet of Things [Ash09; AIM10]
  - Wearables [Man97; MH07]
  - Cyber-Physical Systems [Lee06; RLS+10]

Introdução

Em 1991, Mark Weiser descreveu uma visão do *computador para o século 21* [Wei91]

- Ubiquitous Computing (UbiComp) [Wei93; LY02]
  - Wireless Sensor Networks [EGH+99; PK00]
  - Internet of Things [Ash09; AIM10]
  - Wearables [Man97; MH07]
  - Cyber-Physical Systems [Lee06; RLS+10]

Entretanto,

um quarto de século depois, o sonho de Weiser está longe de se tornar verdadeiro, devido a questões de segurança e privacidade.

Tópicos abordados

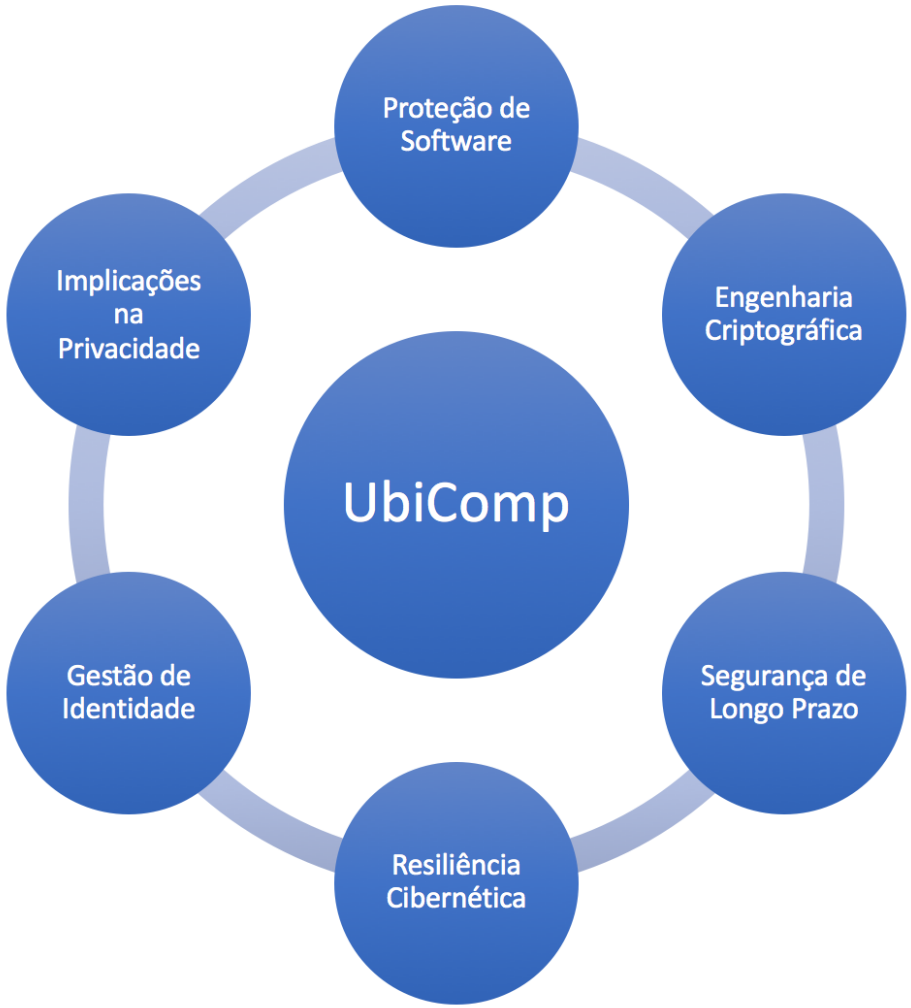
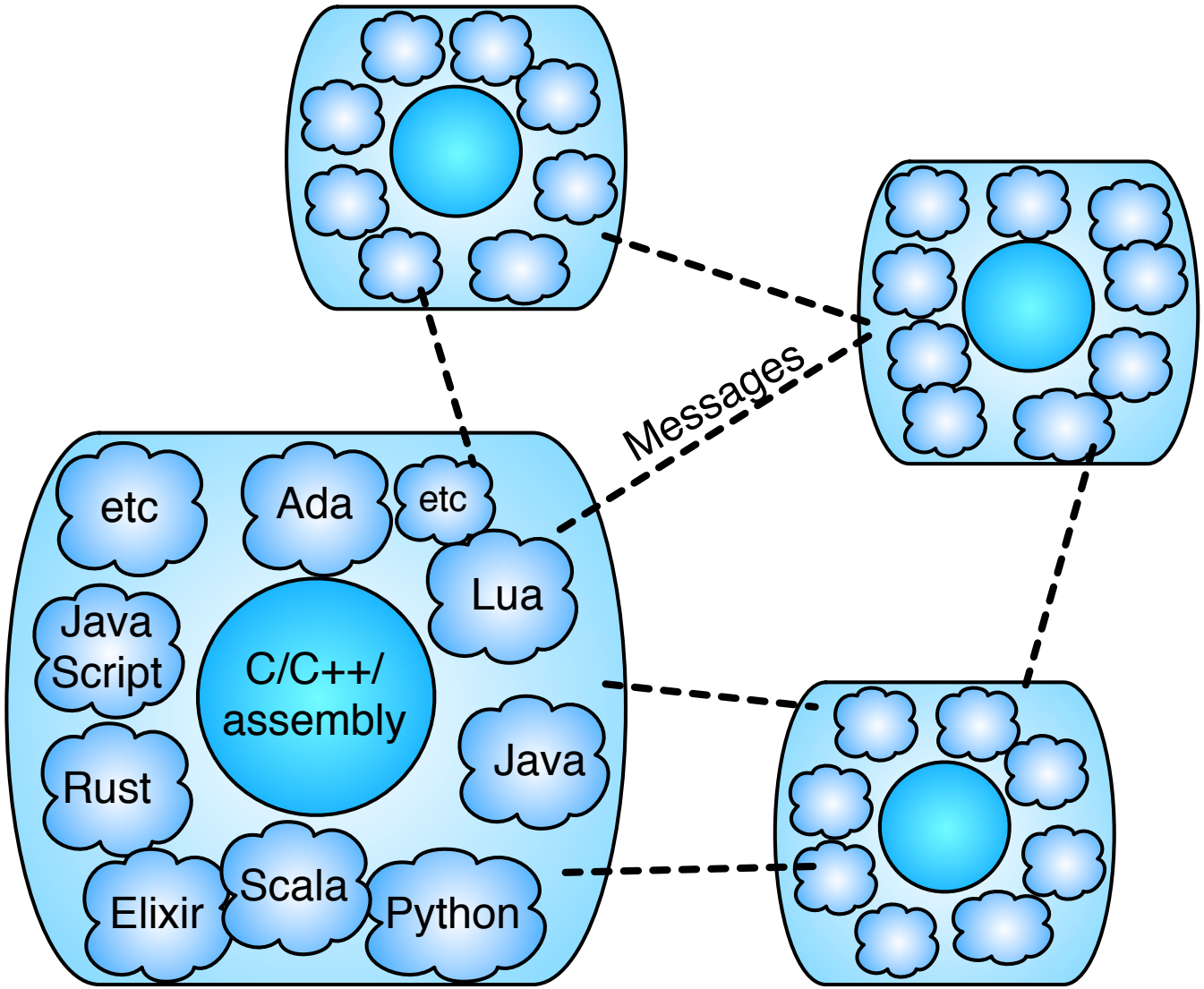


Table of Contents

Ecosistema


Messages
etc
Ada
etc
Lua
Java Script
C/C++/ assembly
Java
Rust
Elixir
Scala
Python

Desafios

- Segurança de tipos

Desafios

- Segurança de tipos
- Programação poliglota

Desafios

- Segurança de tipos
- Programação poliglota
- Programação distribuída

Desafios

- Segurança de tipos
- Programação poliglota
- Programação distribuída

Desafios

- Segurança de tipos
- Programação poliglota
- Programação distribuída

C

```c
#include <stdio.h>
# include <lua5.2/lua.hpp>
// Reads data from Lua, and then sends data to it.
int hello(lua_State* state) {
  int args = lua_gettop(state);
  printf("hello() was called with %d arguments:\n", args);
  for ( int n=1; n<=args; ++n) {
    printf("  arg %d: '%s'\n", n, lua_tostring(state, n));
  }
  lua_pushnumber(state, 123);
  return 1;
}
// Register a call-back function and invoke a Lua program to run it
void execute(const char* filename) {
  lua_State *state = luaL_newstate();
  luaL_openlibs(state);
  lua_register(state, "hello", hello);
  int result = luaL_loadfile(state, filename);
  result = lua_pcall(state, 0, LUA_MULTRET, 0);
}
int main(int argc, char** argv) {
  for (int n=1; n<argc; ++n) { execute(argv[n]); }
}
```

Lua

```lua
io.write("Calling hello() ...\n")
local value = hello("First", "Second", 112233)
io.write(string.format("hello() returned: %s\n", tostring(value)))
```

Table of Contents

Desafios

- Avanços em criptoanálise clássica

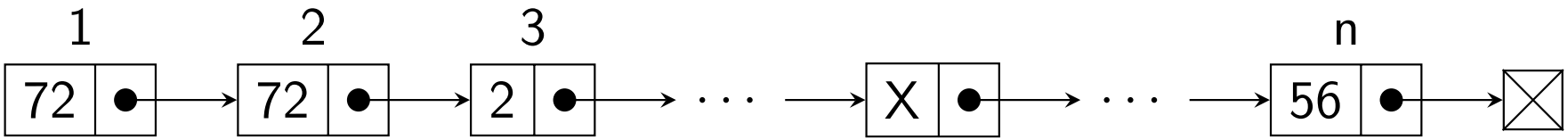
Desafios

- Avanços em criptoanálise clássica
  - caso WPA (Wi-Fi Protected Access)
    "The 4-way handshake was mathematically proven as secure. How is your attack possible?" https://www.krackattacks.com/

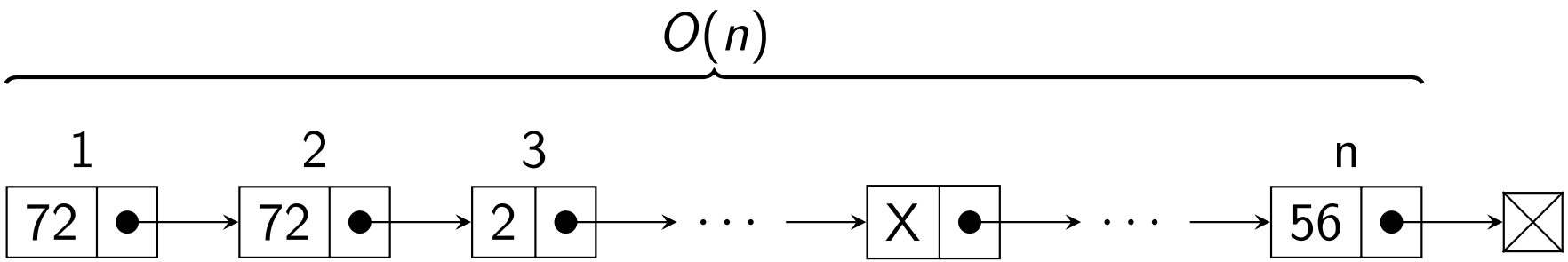
Desafios

- Avanços em criptoanálise clássica
  - caso WPA (Wi-Fi Protected Access)
    “The 4-way handshake was mathematically proven as secure. How is your attack possible?” https://www.krackattacks.com/
- Futura disrupção devido a ataques quânticos [Gro96; Sho97]

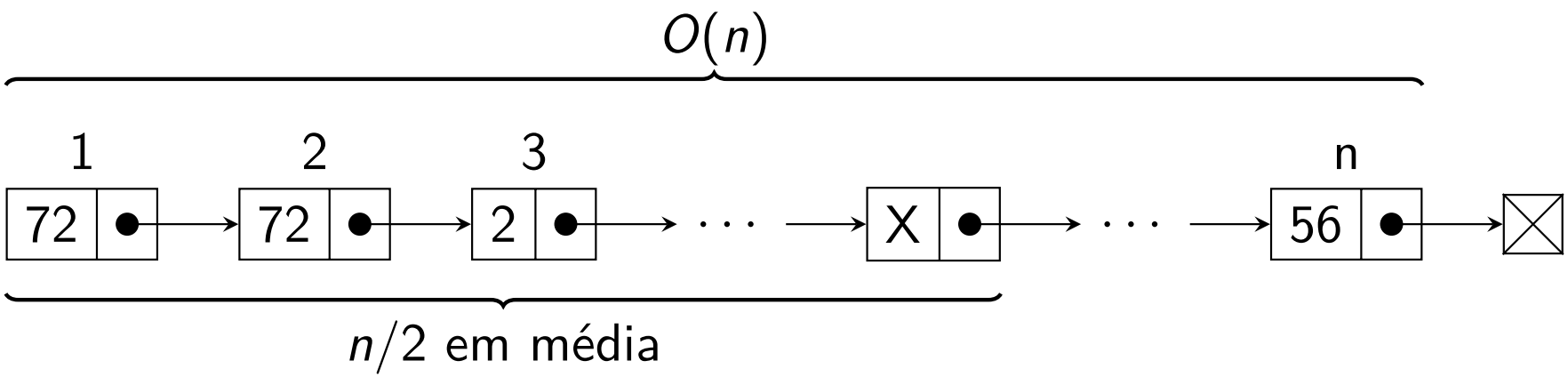
Busca não ordenada



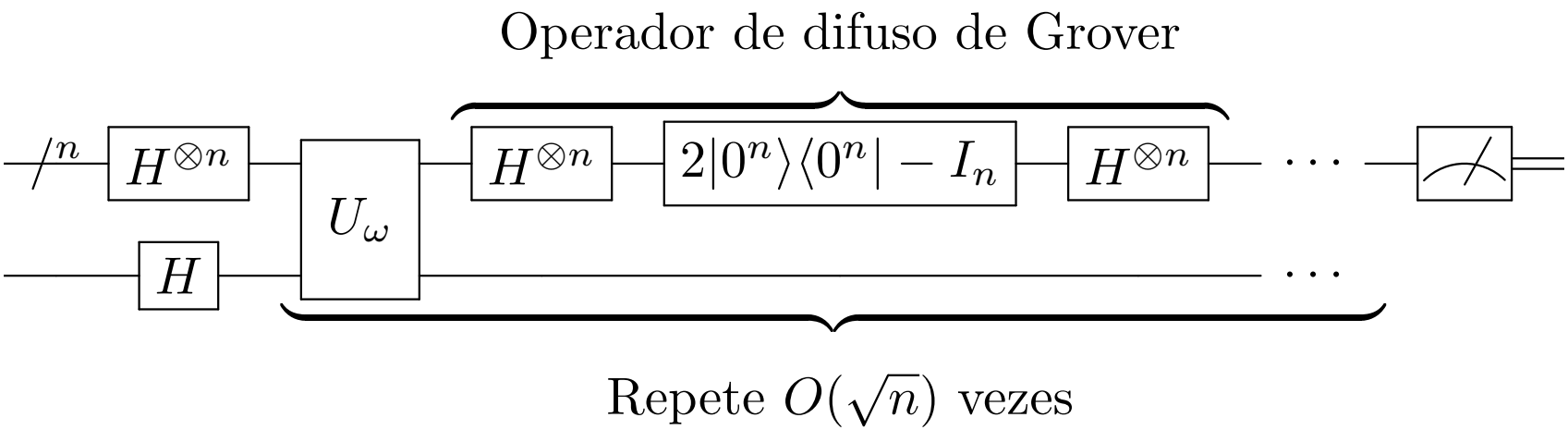
Busca não ordenada



Busca não ordenada



Algoritmo de Grover



Segurança Clássica vs. Quântica

Níveis de Segurança para Criptografia Simétrica

Algoritmo	**Clássica**	**Quântica**
Cifra de Bloco (n bits)	n	$n/2$
Hash Pré-Imagem (n bits)	n	$n/2$
Hash Colisão (n bits)	$n/2$	$n/3$

General number field sieve (GNFS)

tempo sub-exponencial

$$\exp\left(\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right)=L_n\left[\frac{1}{3},\sqrt[3]{\frac{64}{9}}\right]$$

Algoritmo de Shor

$O((\log n)^2(\log\log n)(\log\log\log n))$

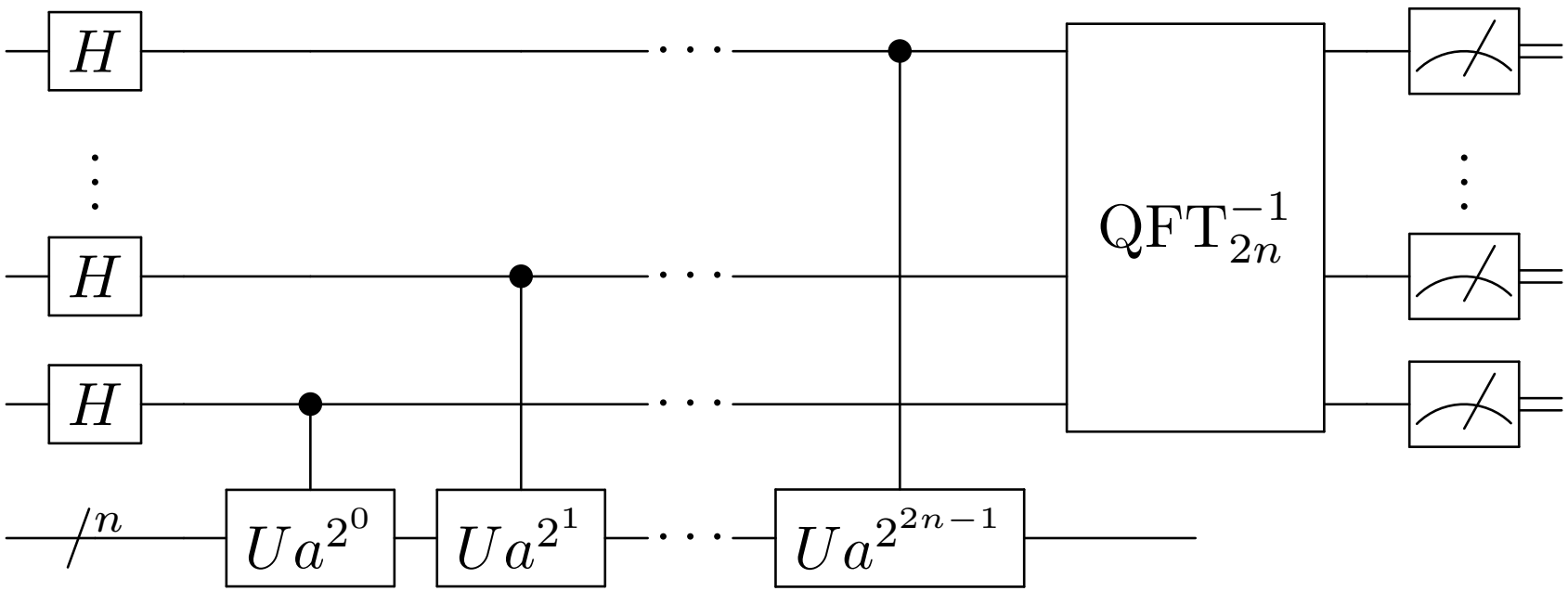
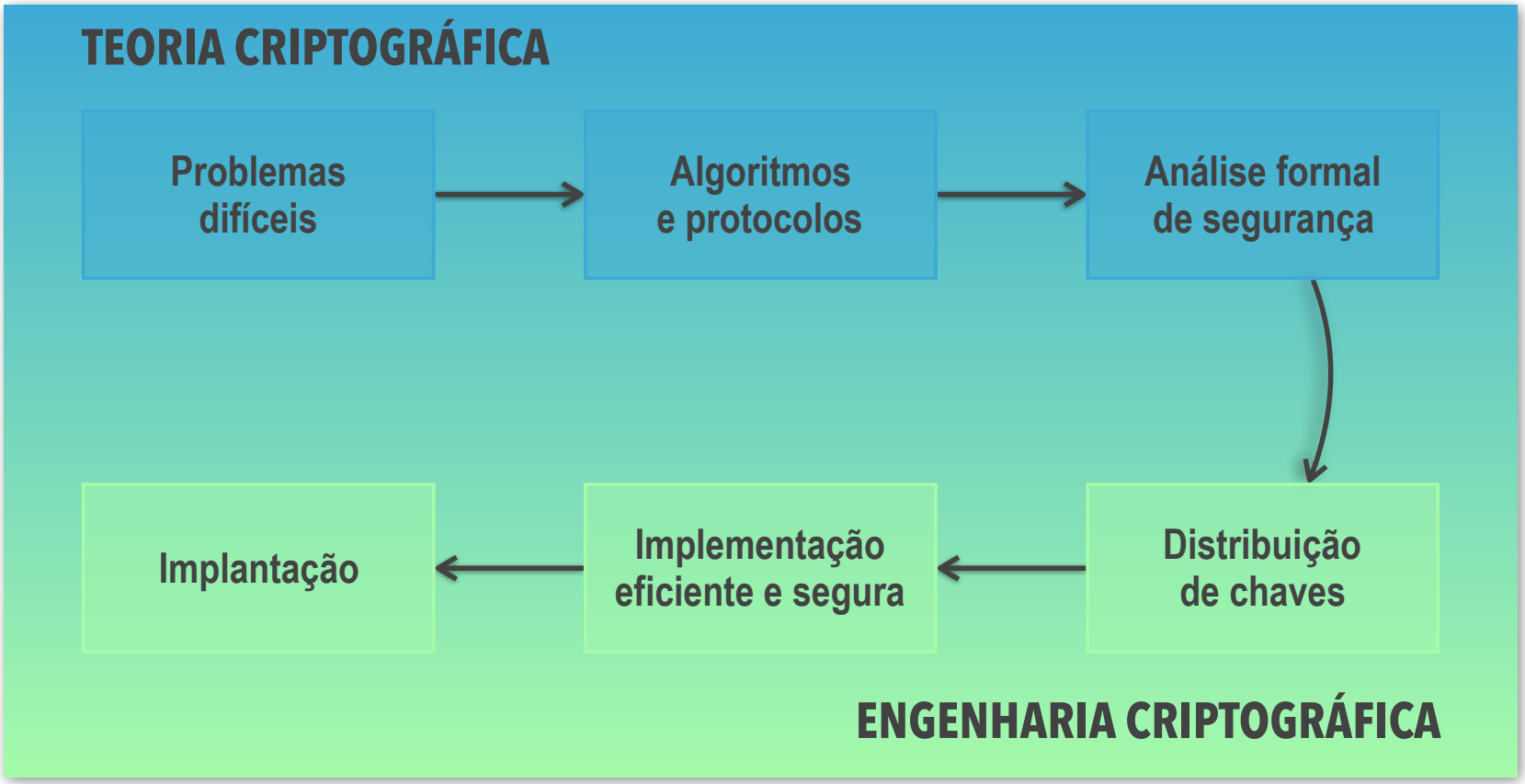


Table of Contents

Tópicos abordados



Desafios

- Geração de chaves

Desafios

- Geração de chaves
- Distribuição de chaves

Desafios

- Geração de chaves
- Distribuição de chaves
- Gerência de chaves

Desafios

- Geração de chaves
- Distribuição de chaves
- Gerência de chaves
  - Eficiência

Desafios

- Geração de chaves
- Distribuição de chaves
- Gerência de chaves
  - Eficiência
  - Funcionalidade

Desafios

- Geração de chaves
- Distribuição de chaves
- Gerência de chaves
  - Eficiência
  - Funcionalidade
  - Comunicação

Desafios

- Geração de chaves
- Distribuição de chaves
- Gerência de chaves
  - Eficiência
  - Funcionalidade
  - Comunicação
  - Interoperabilidade

Desafios

- Geração de chaves
- Distribuição de chaves
- Gerência de chaves
  - Eficiência
  - Funcionalidade
  - Comunicação
  - Interoperabilidade
- Criptografia leve

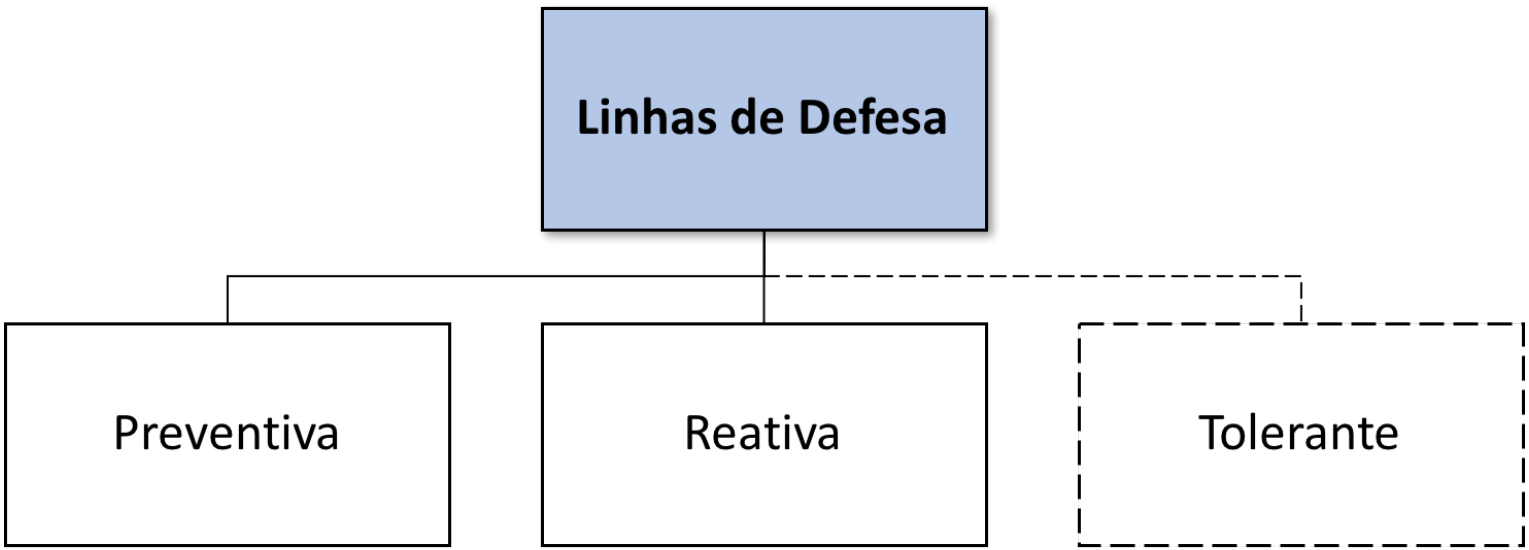
Desafios

- Geração de chaves
- Distribuição de chaves
- Gerência de chaves
  - Eficiência
  - Funcionalidade
  - Comunicação
  - Interoperabilidade
- Criptografia leve
- Resistência a ataques de canal lateral

Table of Contents

Linhas de Defesa

Composição da Resiliência [Nog09]



Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração
- autoadaptação

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração
- autoadaptação
- eficiência

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração
- autoadaptação
- eficiência
- controle de acesso

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração
- autoadaptação
- eficiência
- controle de acesso
- proteção

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração
- autoadaptação
- eficiência
- controle de acesso
- proteção
- integridade, confidencialidade e não-repúdio

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração
- autoadaptação
- eficiência
- controle de acesso
- proteção
- integridade, confidencialidade e não-repúdio
- redundância

Serviços essenciais

Requisitos de resiliência no contexto UbiComp

- heterogeneidade
- autoconfiguração
- autoadaptação
- eficiência
- controle de acesso
- proteção
- integridade, confidencialidade e não-repúdio
- redundância
- robustez

Redes ou sistema

Requisitos de resiliência no contexto UbiComp

- descentralização

Redes ou sistema

Requisitos de resiliência no contexto UbiComp

- descentralização
- auto-organização

Redes ou sistema

Requisitos de resiliência no contexto UbiComp

- descentralização
- auto-organização
- escalabilidade

Redes ou sistema

Requisitos de resiliência no contexto UbiComp

- descentralização
- auto-organização
- escalabilidade
- autodiagnóstico

Redes ou sistema

Requisitos de resiliência no contexto UbiComp

- descentralização
- auto-organização
- escalabilidade
- autodiagnóstico
- autorrecuperação

Redes ou sistema

Requisitos de resiliência no contexto UbiComp

- descentralização
- auto-organização
- escalabilidade
- autodiagnóstico
- autorrecuperação
- auto-otimização

Desafios

- Integração dos requisitos

Desafios

- Integração dos requisitos
- Escalabilidade

Desafios

- Integração dos requisitos
- Escalabilidade
- Incertezas sobre os sistemas

Desafios

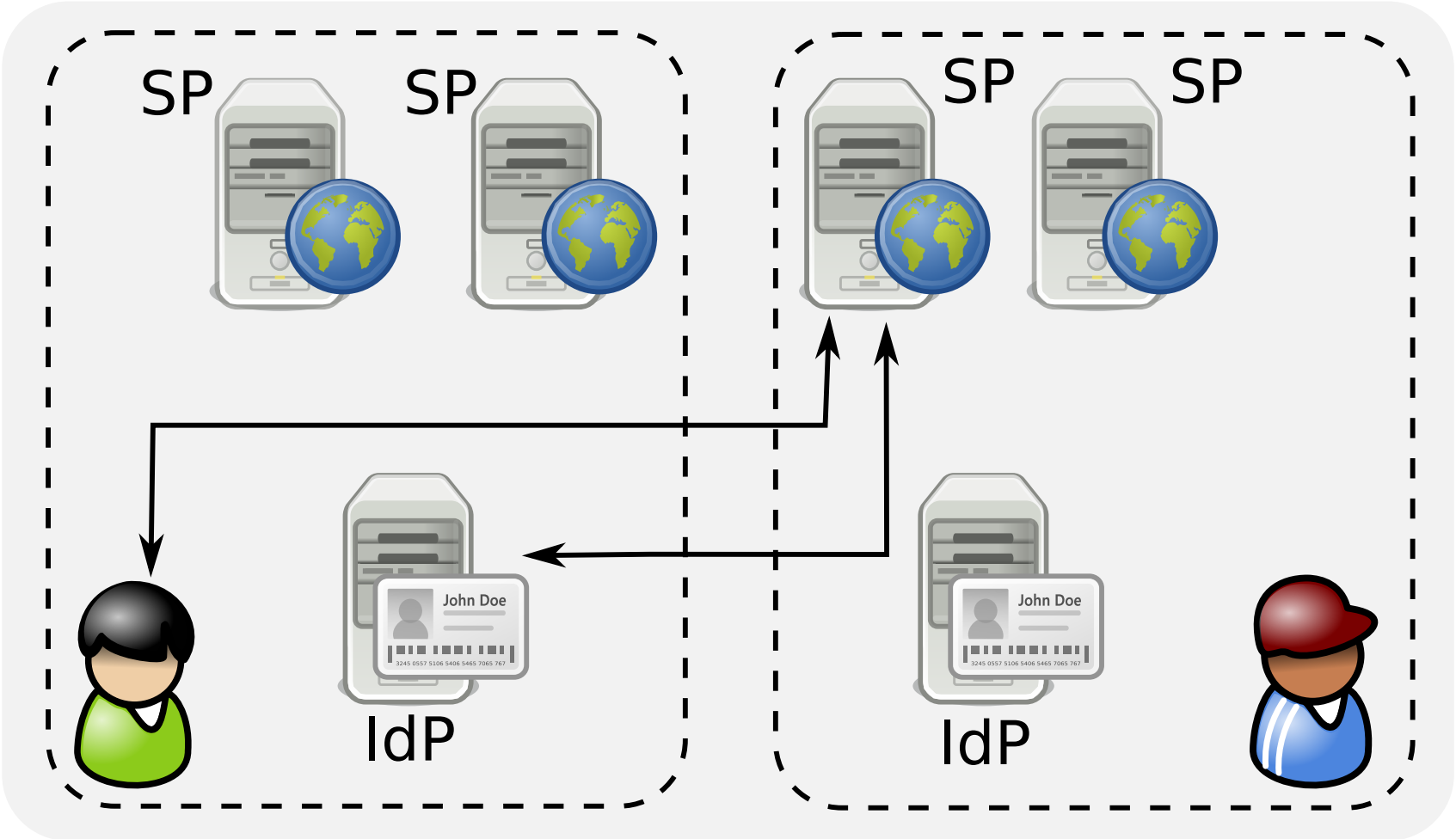
- Integração dos requisitos
- Escalabilidade
- Incertezas sobre os sistemas
- Baixo tempo de resposta

Desafios

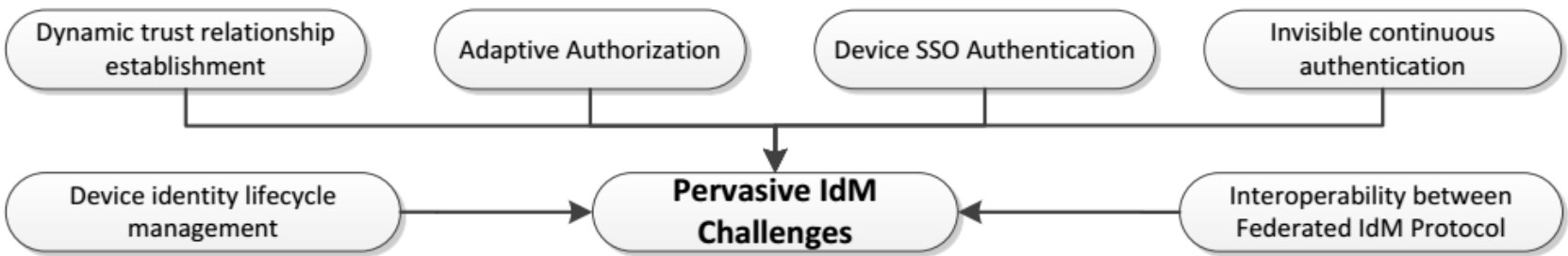
- Integração dos requisitos
- Escalabilidade
- Incertezas sobre os sistemas
- Baixo tempo de resposta
- Coordenar de forma adaptativa as três linhas de defesa

Table of Contents

Modelo de Identidades Federadas



Pervasive IdM Challenges



Desafios

- Autenticação

Desafios

- Autenticação
- Autorização

Desafios

- Autenticação
- Autorização
- Protocolos de Gestão de Identidade Federada

Desafios

- Autenticação
- Autorização
- Protocolos de Gestão de Identidade Federada
- Outros Desafios da Gestão de Identidade Pervasiva

Desafios

- Autenticação
- Autorização
- Protocolos de Gestão de Identidade Federada
- Outros Desafios da Gestão de Identidade Pervasiva
  - acordos entre suas entidades (IdPs, SPs)

Desafios

- Autenticação
- Autorização
- Protocolos de Gestão de Identidade Federada
- Outros Desafios da Gestão de Identidade Pervasiva
  - acordos entre suas entidades (IdPs, SPs)
  - interoperabilidade (SAML, OpenId Connect e OAuth)

Desafios

- Autenticação
- Autorização
- Protocolos de Gestão de Identidade Federada
- Outros Desafios da Gestão de Identidade Pervasiva
  - acordos entre suas entidades (IdPs, SPs)
  - interoperabilidade (SAML, OpenId Connect e OAuth)
  - política de privacidade

Table of Contents

Segurança versus Privacidade

Desafios

- Desafios dos cenários de aplicação

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação
- Desafios tecnológicos

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação
- Desafios tecnológicos
  - Computar todos os operadores

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação
- Desafios tecnológicos
  - Computar todos os operadores
  - Trade-off entre garantia e maleabilidade

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação
- Desafios tecnológicos
  - Computar todos os operadores
  - Trade-off entre garantia e maleabilidade
  - Distribuição de chaves

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação
- Desafios tecnológicos
  - Computar todos os operadores
  - Trade-off entre garantia e maleabilidade
  - Distribuição de chaves
  - Agregação e consolidação

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação
- Desafios tecnológicos
  - Computar todos os operadores
  - Trade-off entre garantia e maleabilidade
  - Distribuição de chaves
  - Agregação e consolidação
  - Performance

Desafios

- Desafios dos cenários de aplicação
  - Identificar dados sensíveis
  - Regulamentação
- Desafios tecnológicos
  - Computar todos os operadores
  - Trade-off entre garantia e maleabilidade
  - Distribuição de chaves
  - Agregação e consolidação
  - Performance
  - falhas e rupturas

Base de dados “anônima”

[LLV07]

	CEP	Idade	Doença
1	47677	29	Doenças cardiovasculares
2	47602	22	Doenças cardiovasculares
3	47678	27	Doenças cardiovasculares
4	47905	43	Resfriado
5	47909	52	Doenças cardiovasculares
6	47906	47	Câncer
7	47605	30	Doenças cardiovasculares
8	47673	36	Câncer
9	47607	32	Câncer

Base de dados “anonimizada”

k-Anonymous

	CEP	Idade	Doença
1	476**	2*	Doenças cardiovasculares
2	476**	2*	Doenças cardiovasculares
3	476**	2*	Doenças cardiovasculares
4	4790*	$\geqslant$ 40	Resfriado
5	4790*	$\geqslant$ 40	Doenças cardiovasculares
6	4790*	$\geqslant$ 40	Câncer
7	476**	3*	Doenças cardiovasculares
8	476**	3*	Câncer
9	476**	3*	Câncer

Shannon

Adversário

Remetente

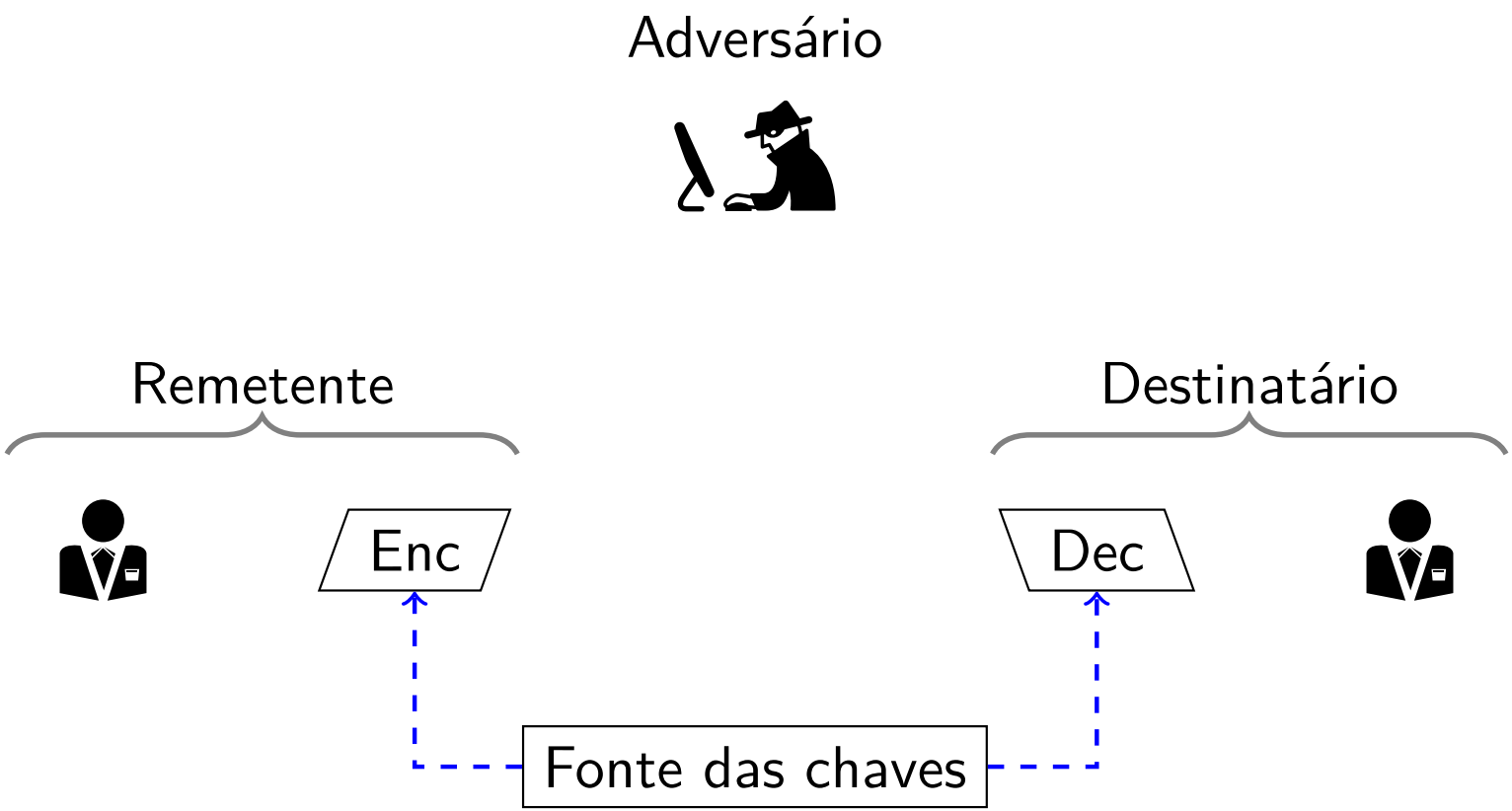
Enc

Destinatário

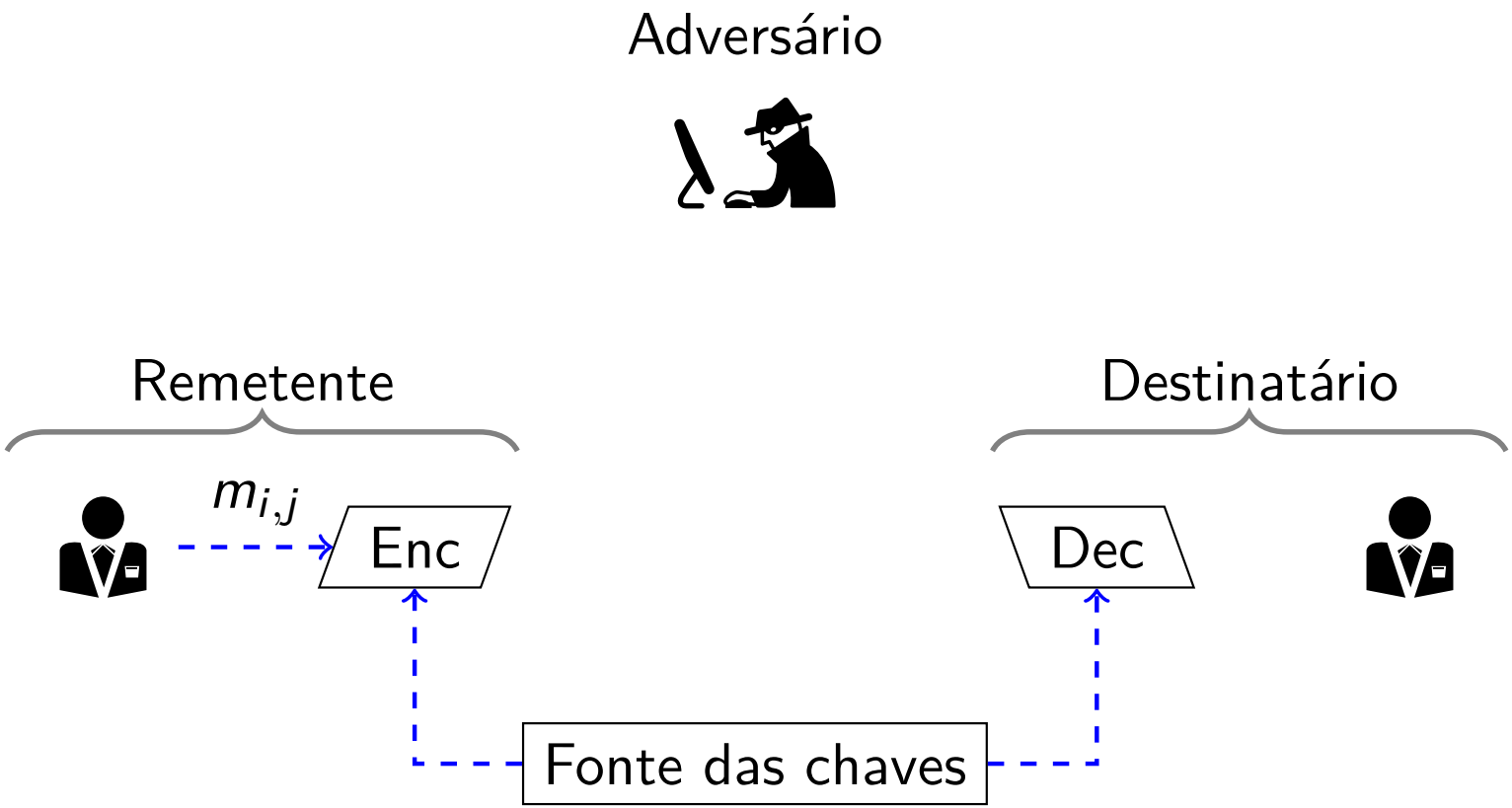
Dec

Fonte das chaves

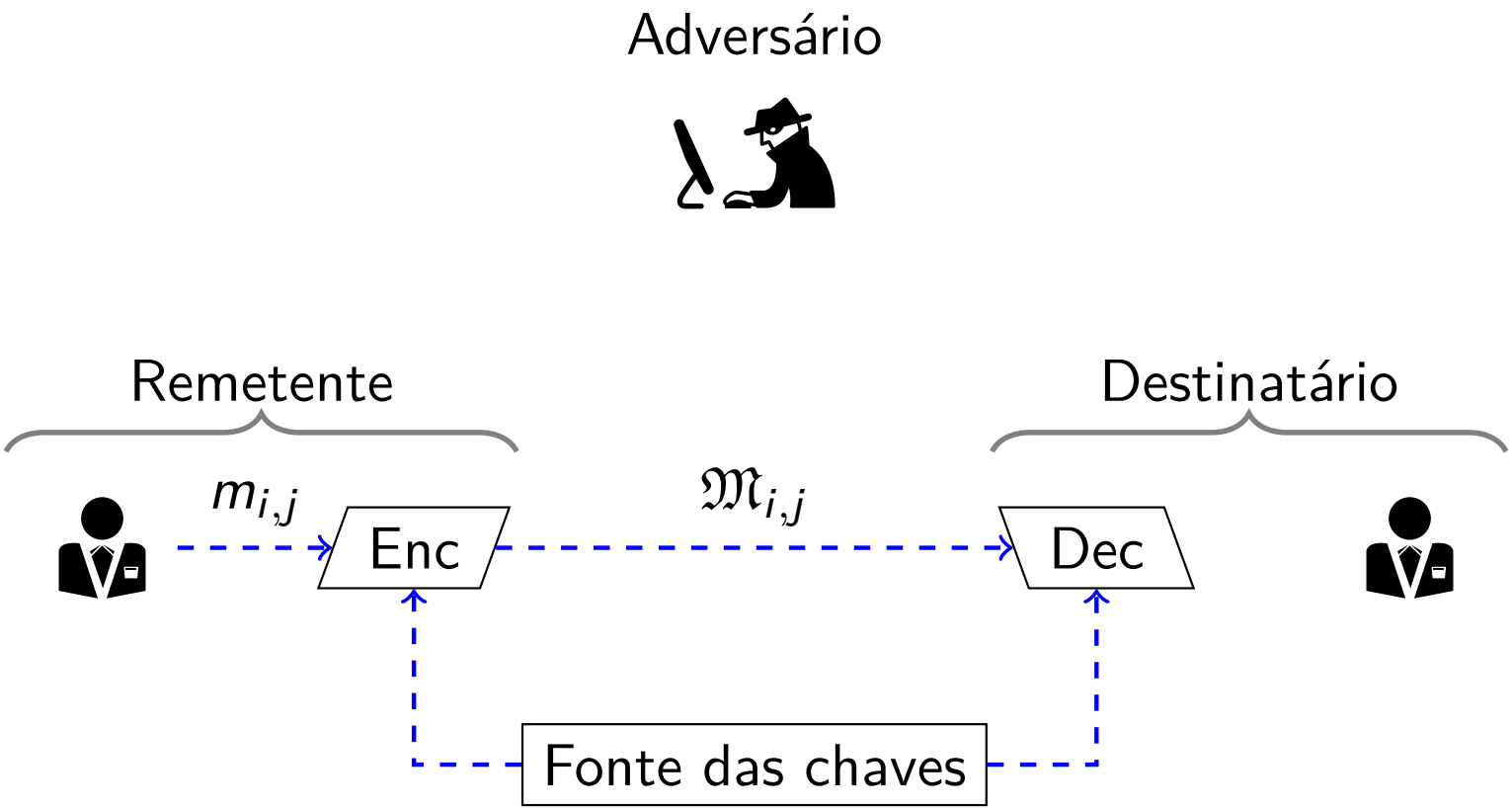
Shannon


Adversário
Remetente
Destinatário
Enc
Dec
Fonte das chaves

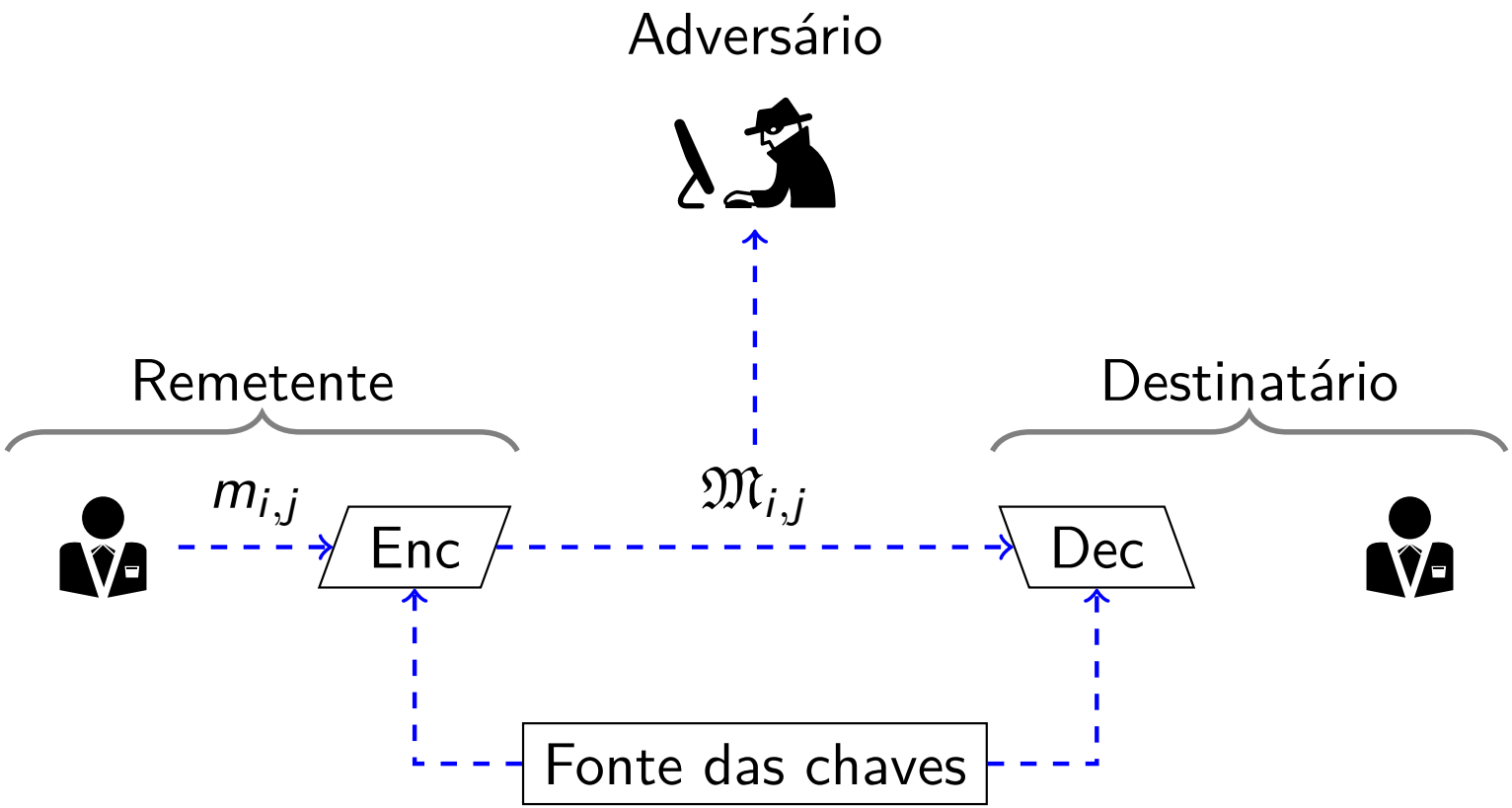
Shannon


Adversário
Remetente
Destinatário
$m_{i,j}$
Enc
Dec
Fonte das chaves

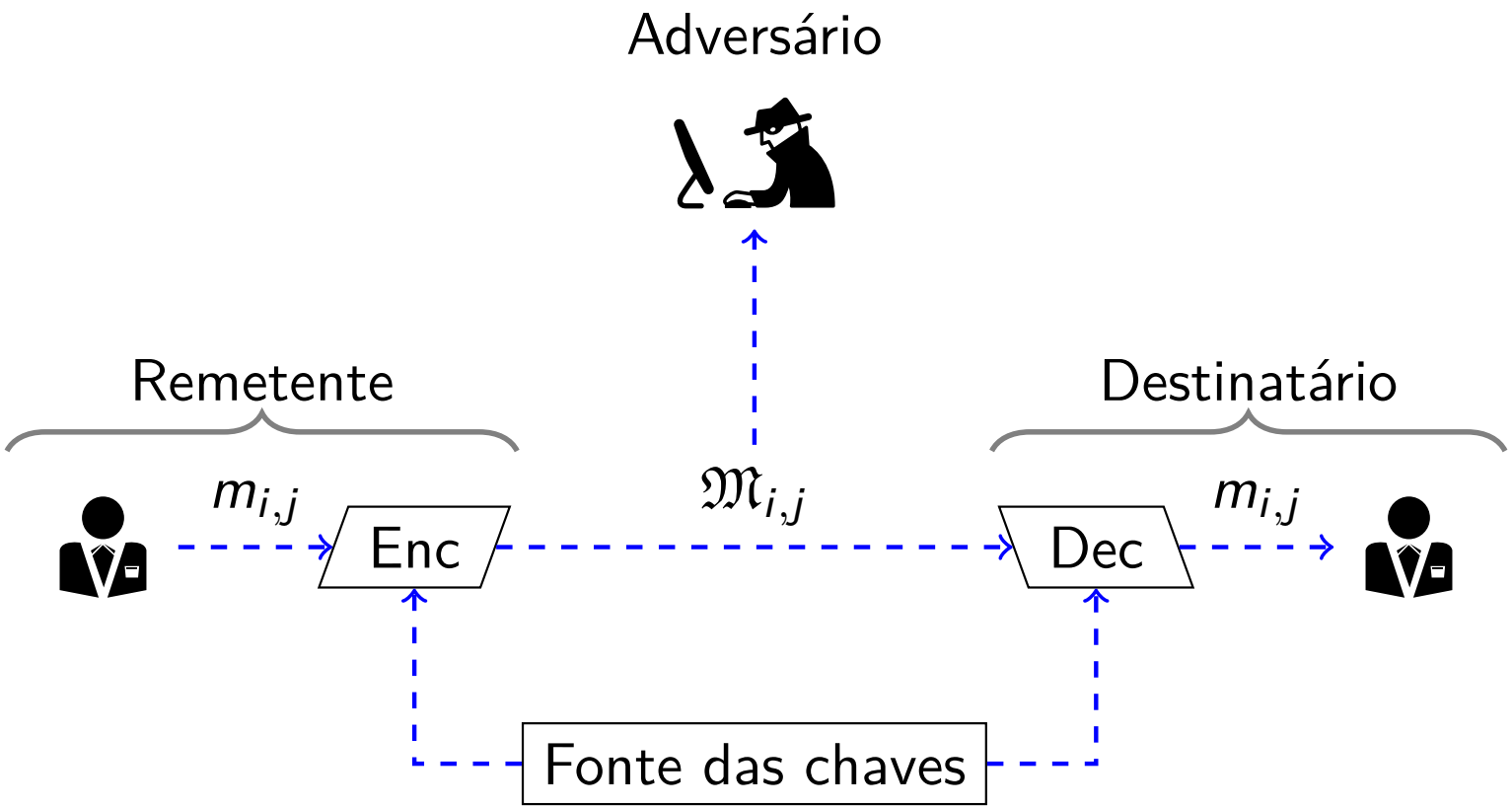
Shannon


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

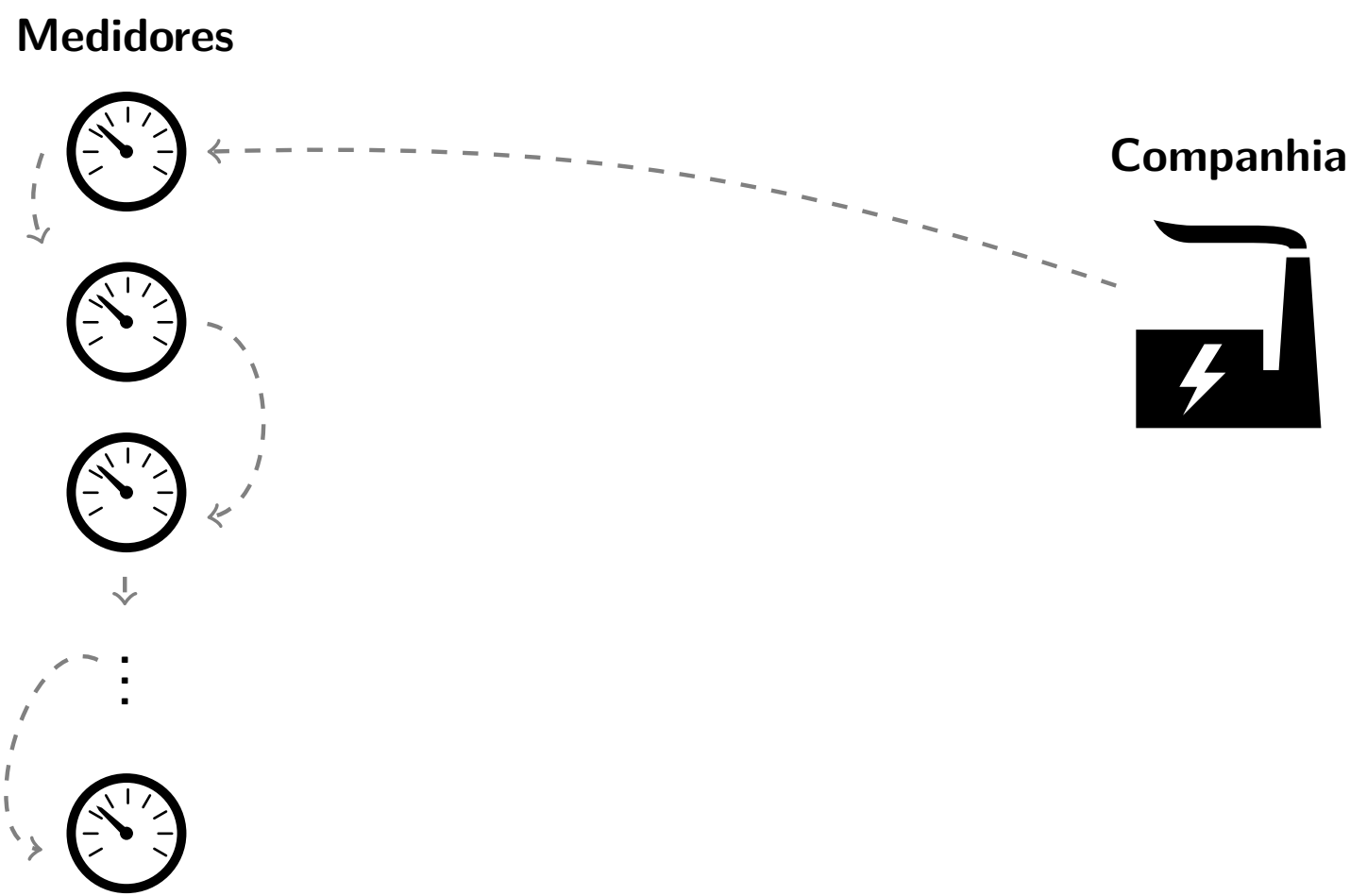
Shannon


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

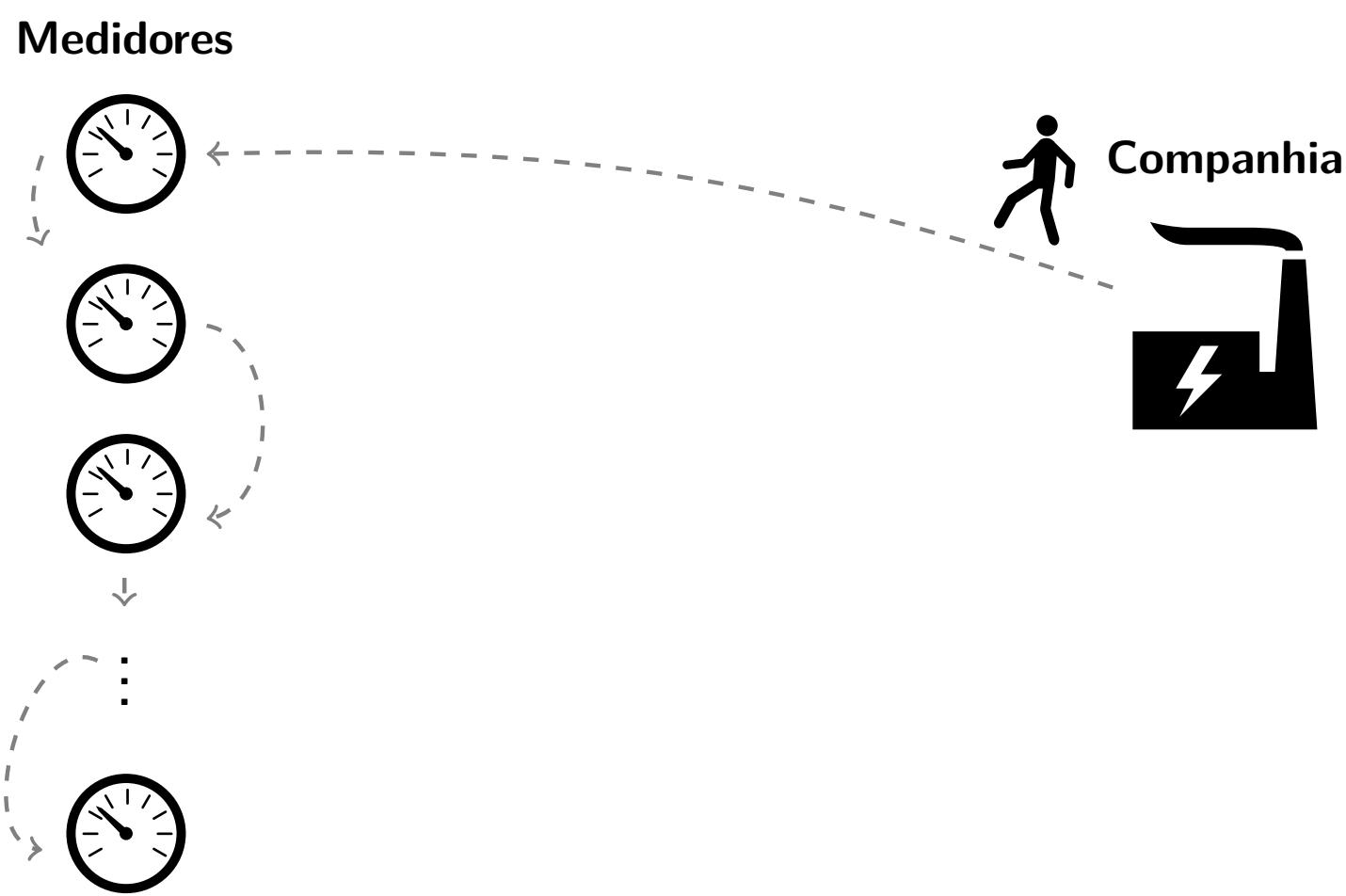
Shannon


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

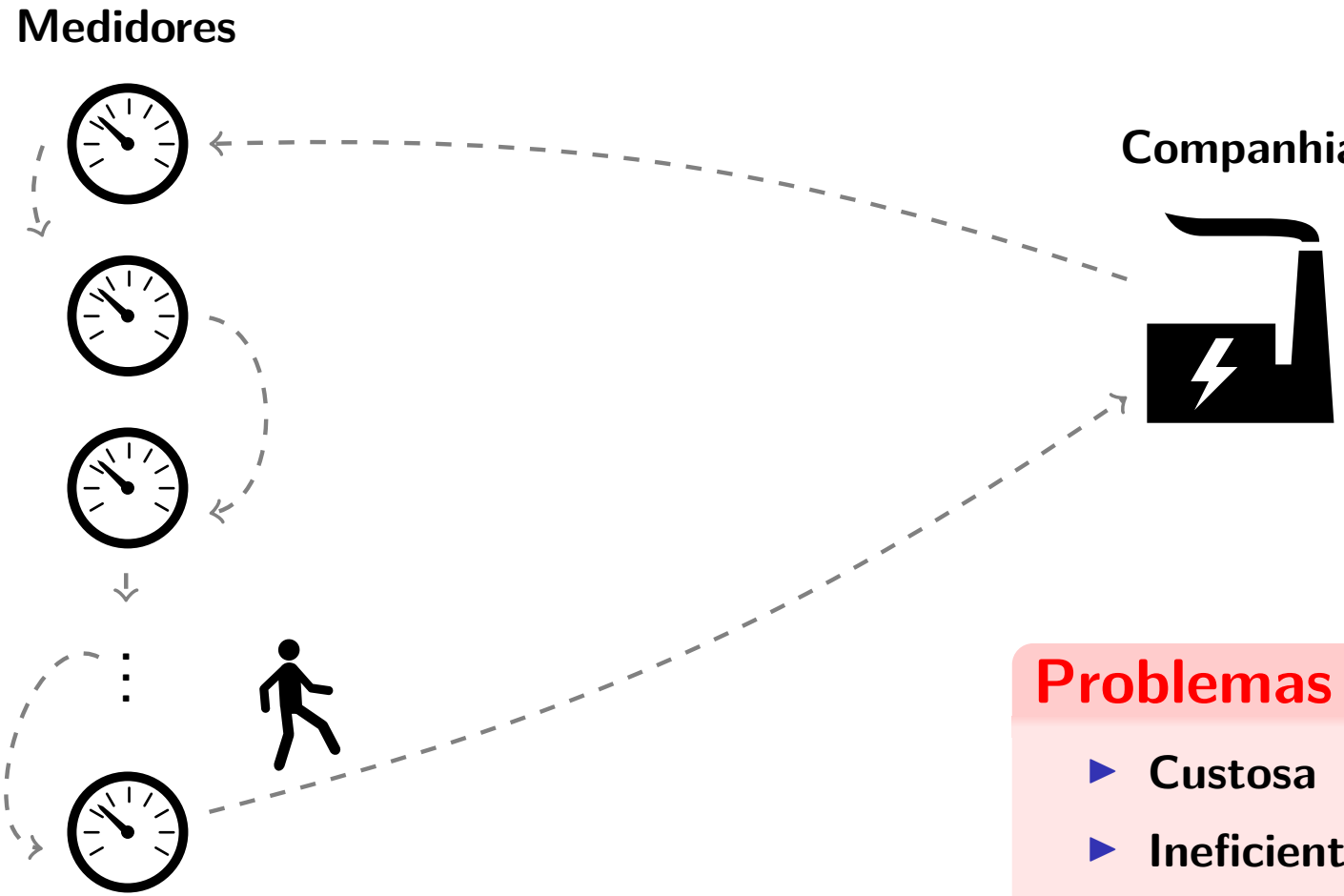
Non-smart Grid



Non-smart Grid



Non-smart Grid

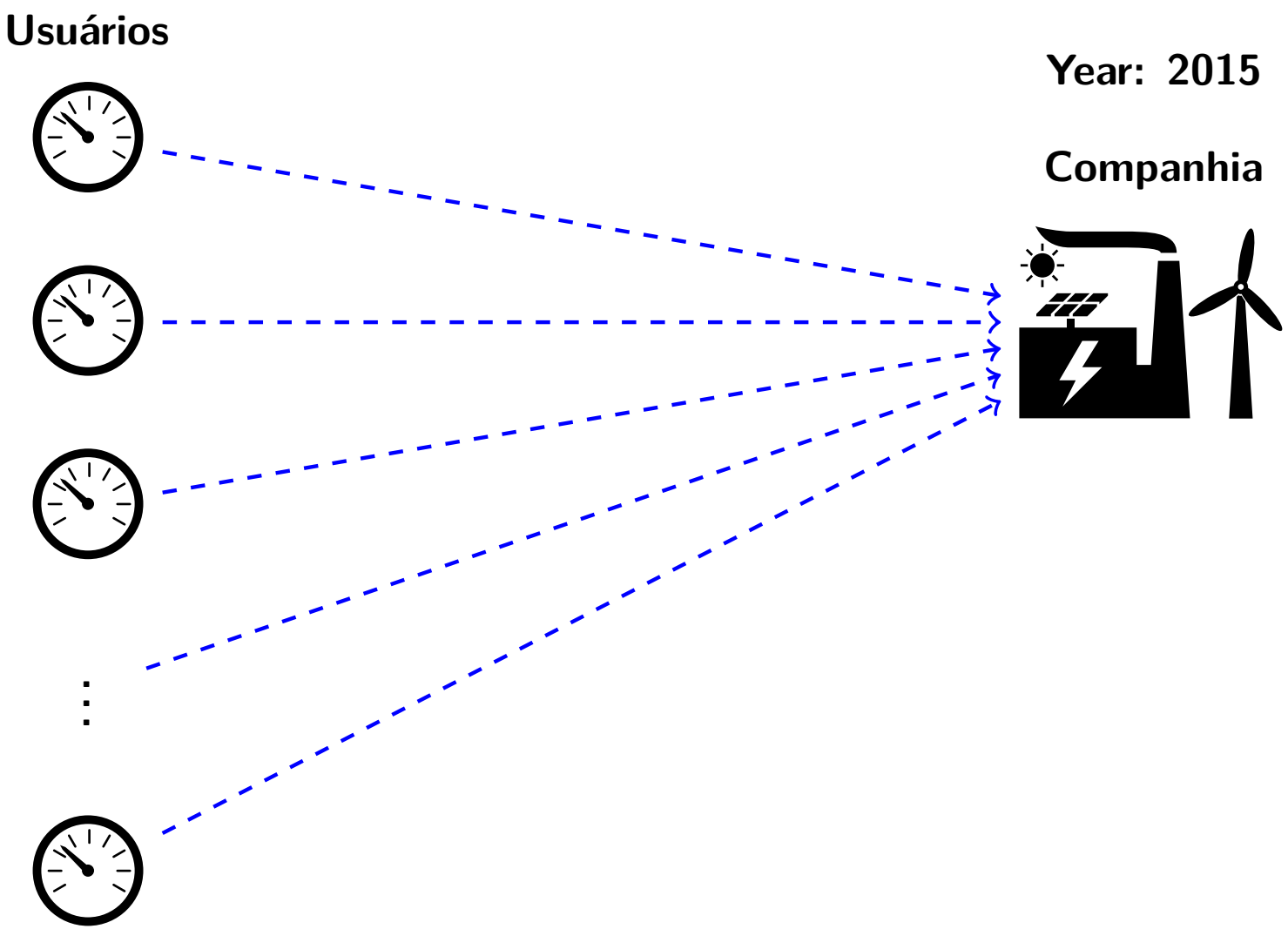


Problemas

- Custosa
- Ineficiente
- Fraudes

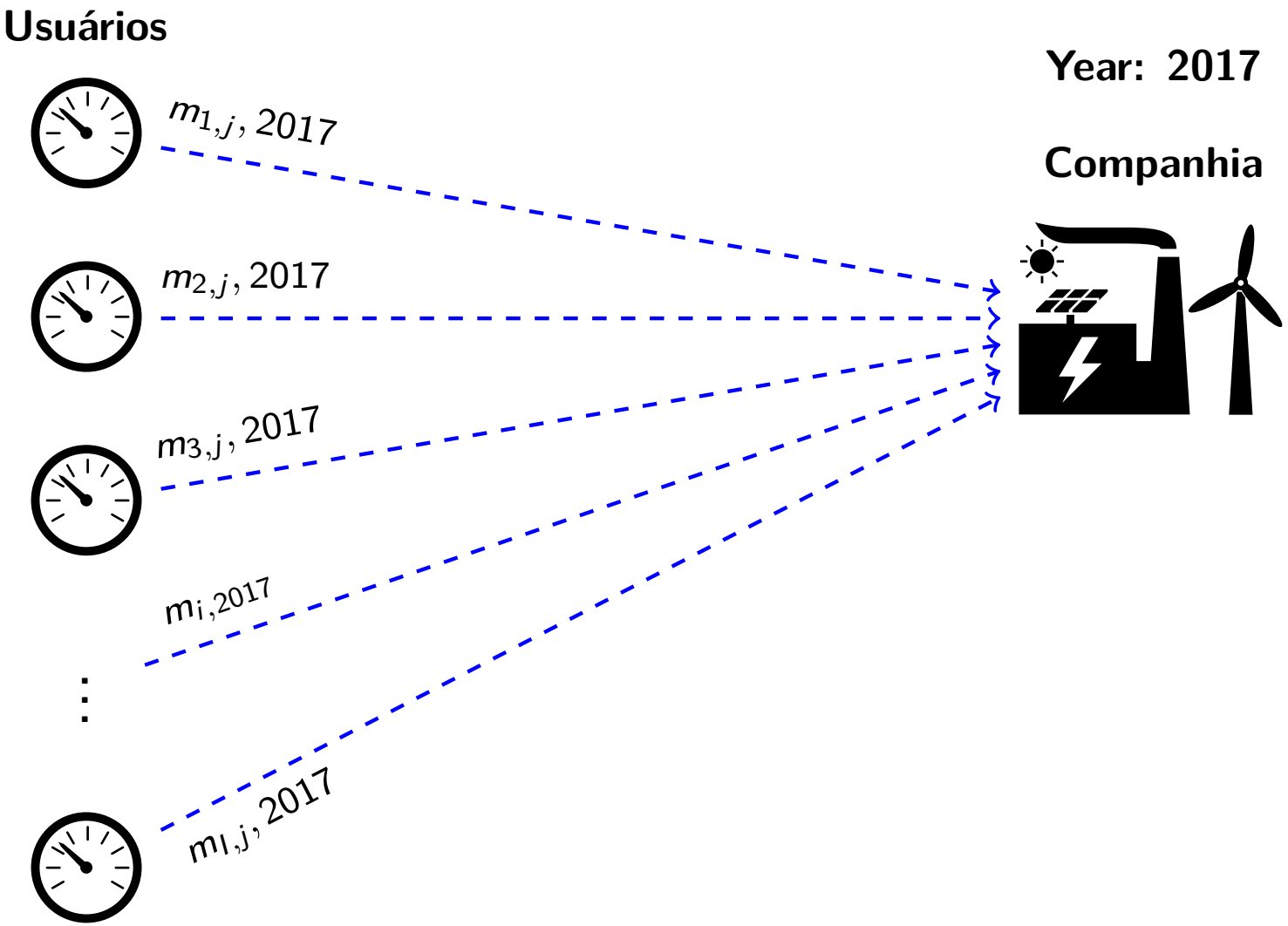
Tornando Inteligente

Coletando medições anualmente



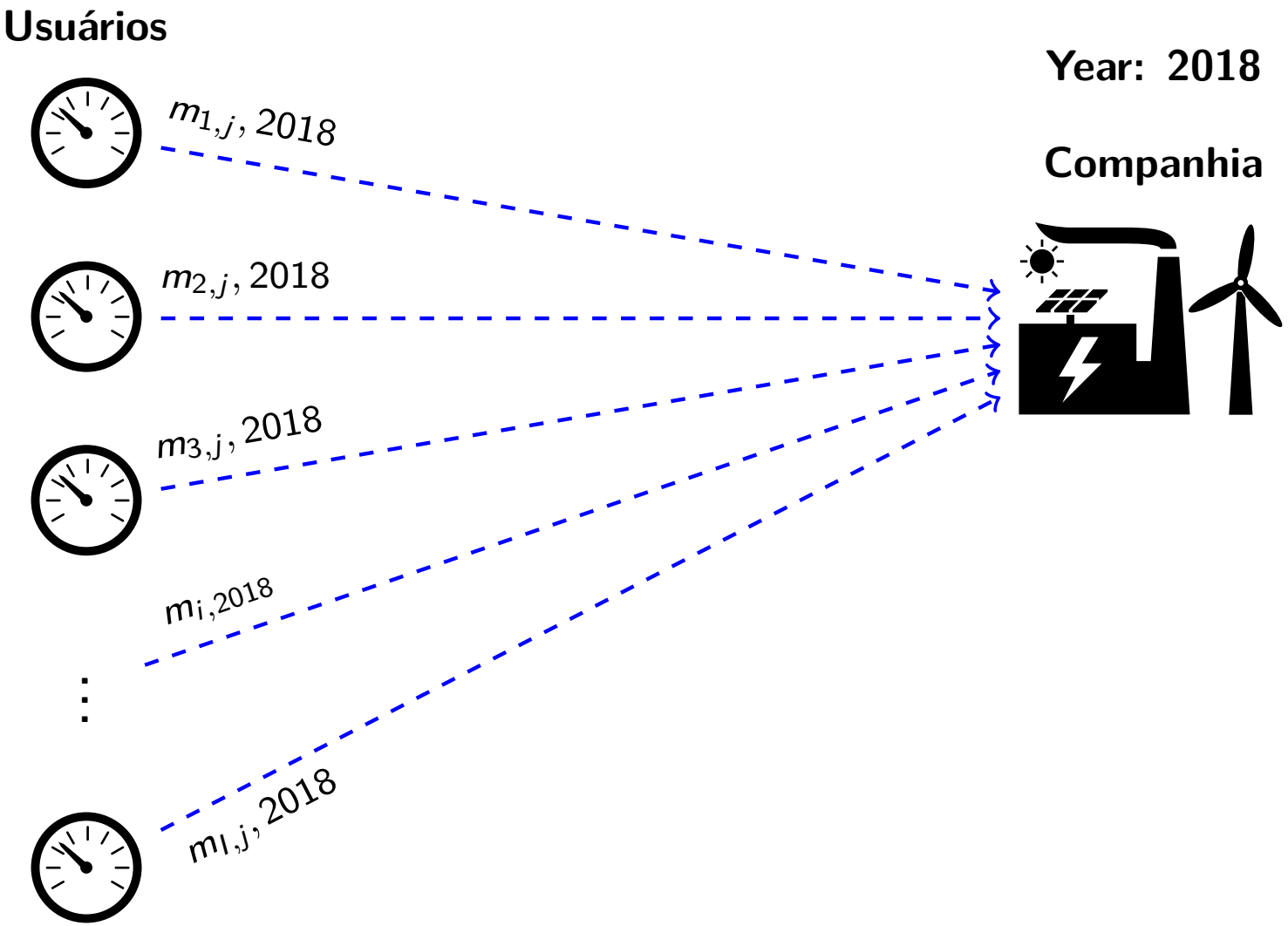
Tornando Inteligente

Coletando medições anualmente



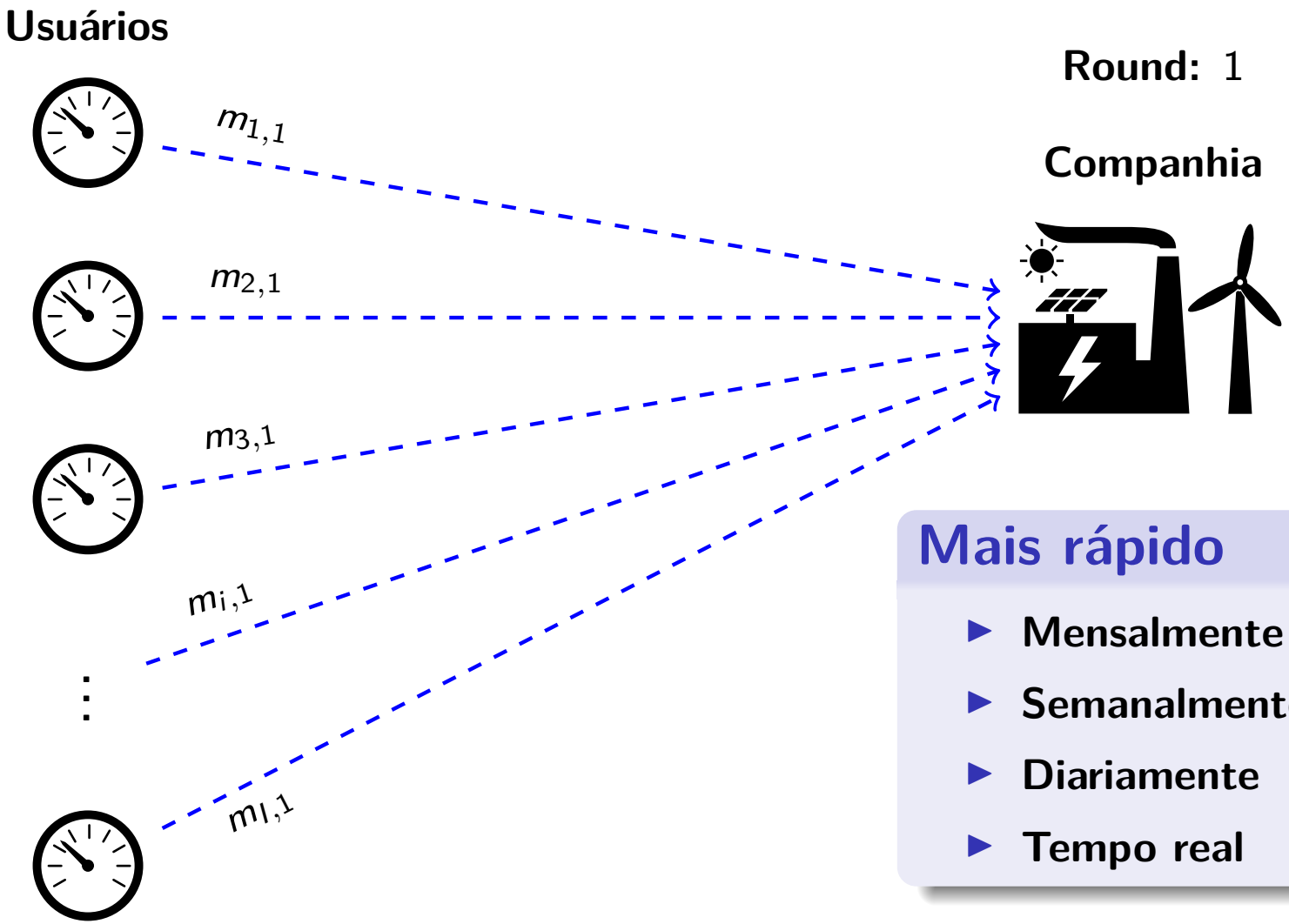
Tornando Inteligente

Coletando medições anualmente



Tornando Inteligente

Coletando medições anualmente

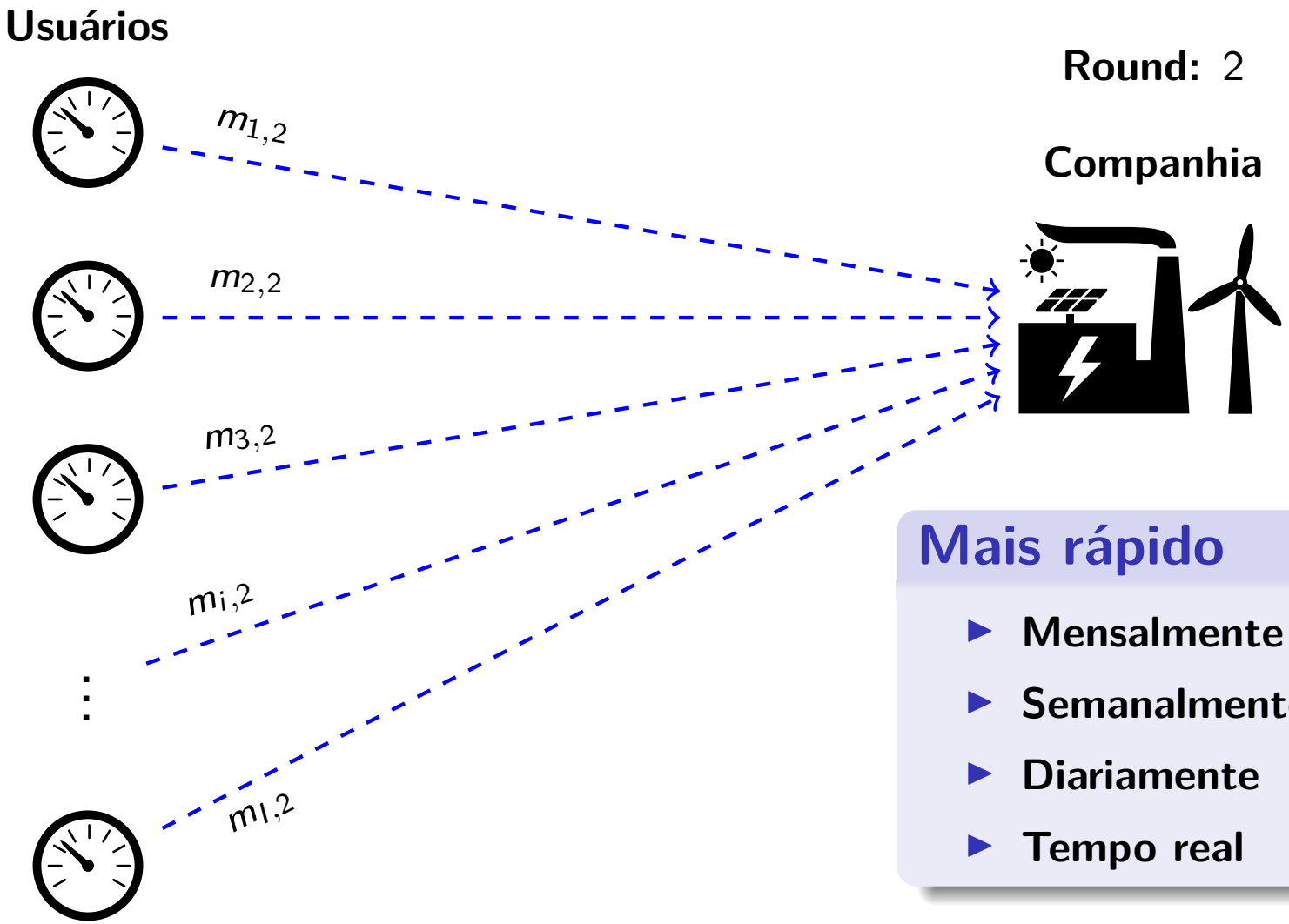


Mais rápido

- Mensalmente
- Semanalmente
- Diariamente
- Tempo real

Tornando Inteligente

Coletando medições anualmente

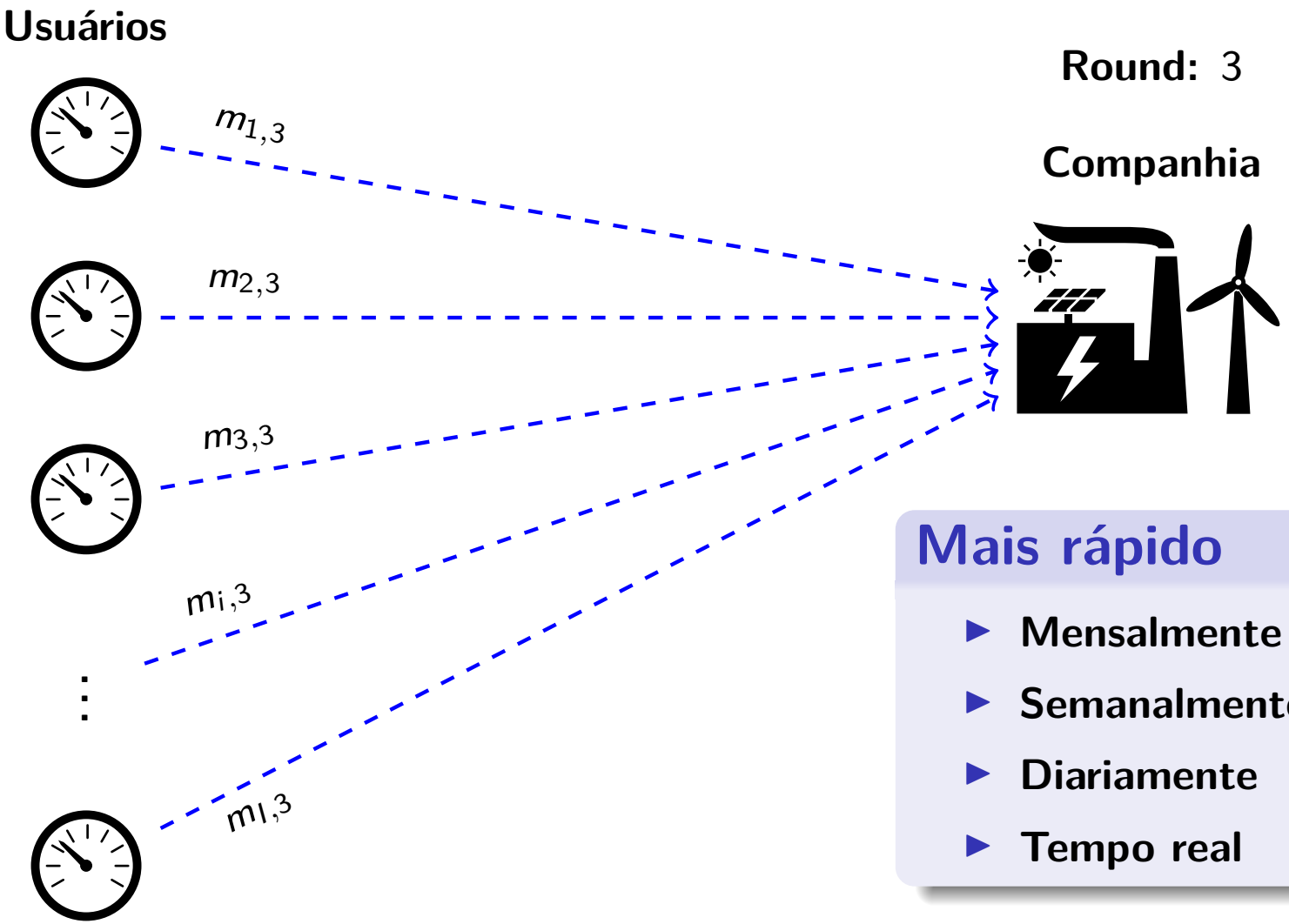


Mais rápido

- Mensalmente
- Semanalmente
- Diariamente
- Tempo real

Tornando Inteligente

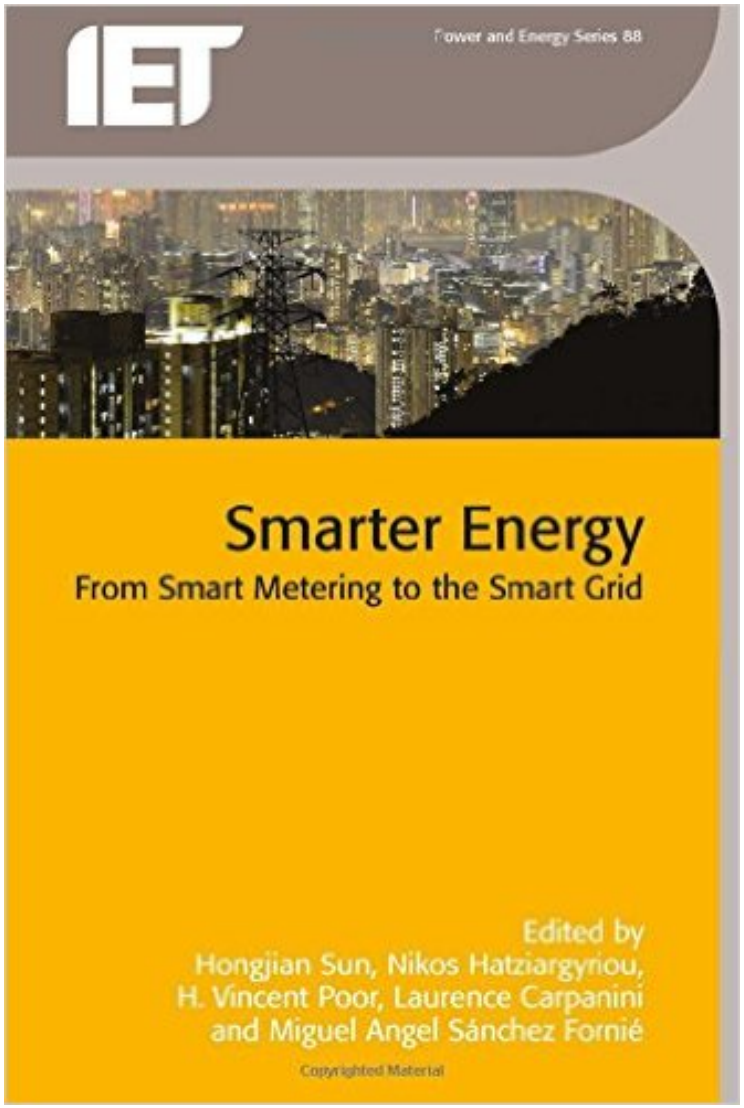
Coletando medições anualmente

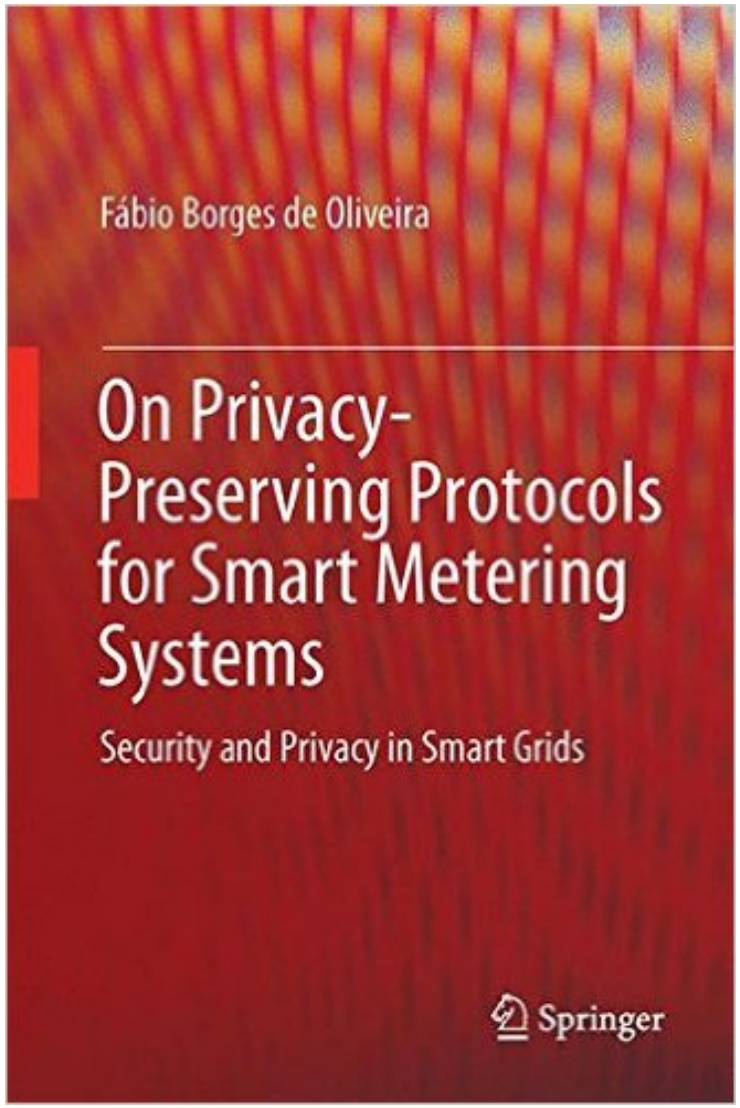


Mais rápido

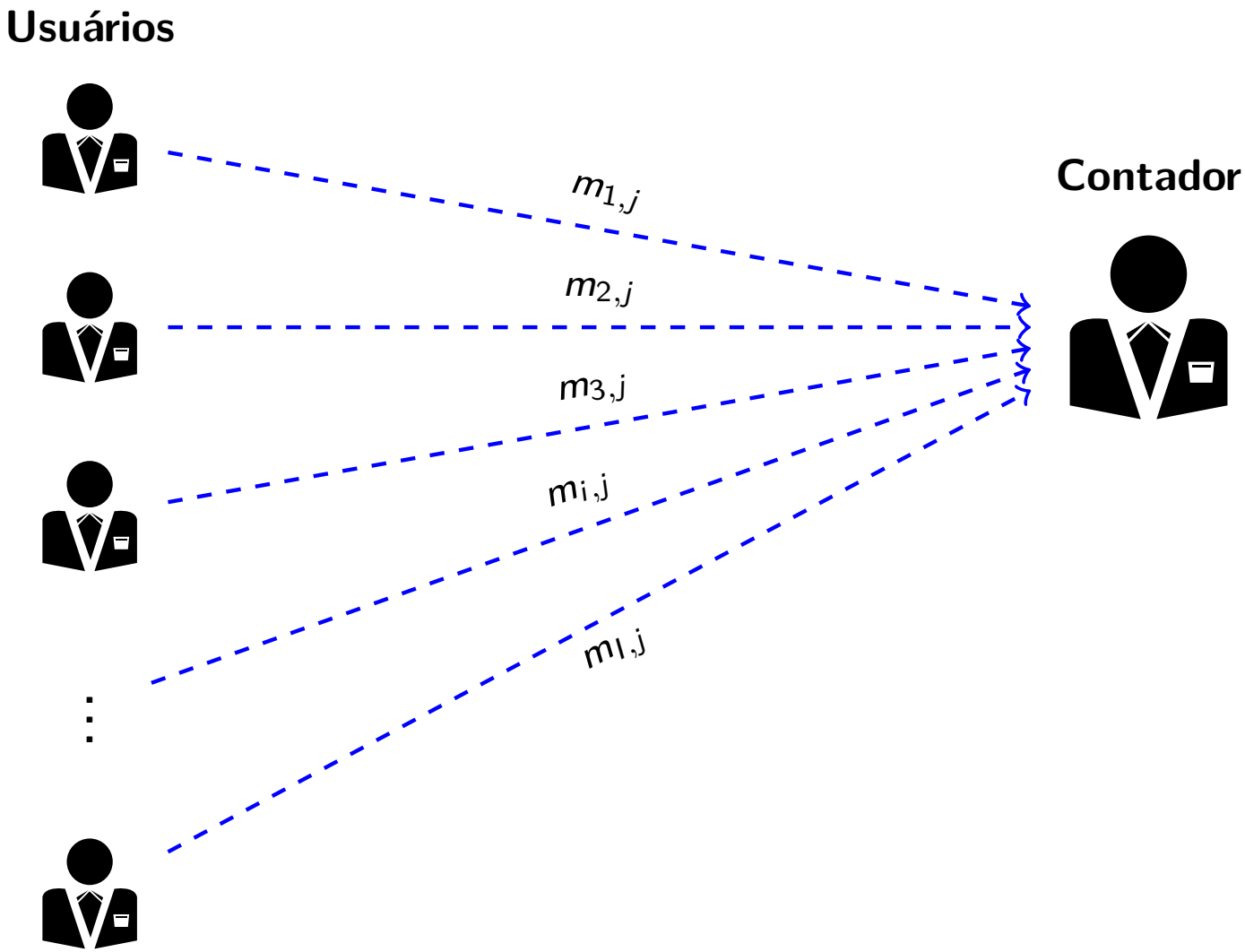
- Mensalmente
- Semanalmente
- Diariamente
- Tempo real

Referências

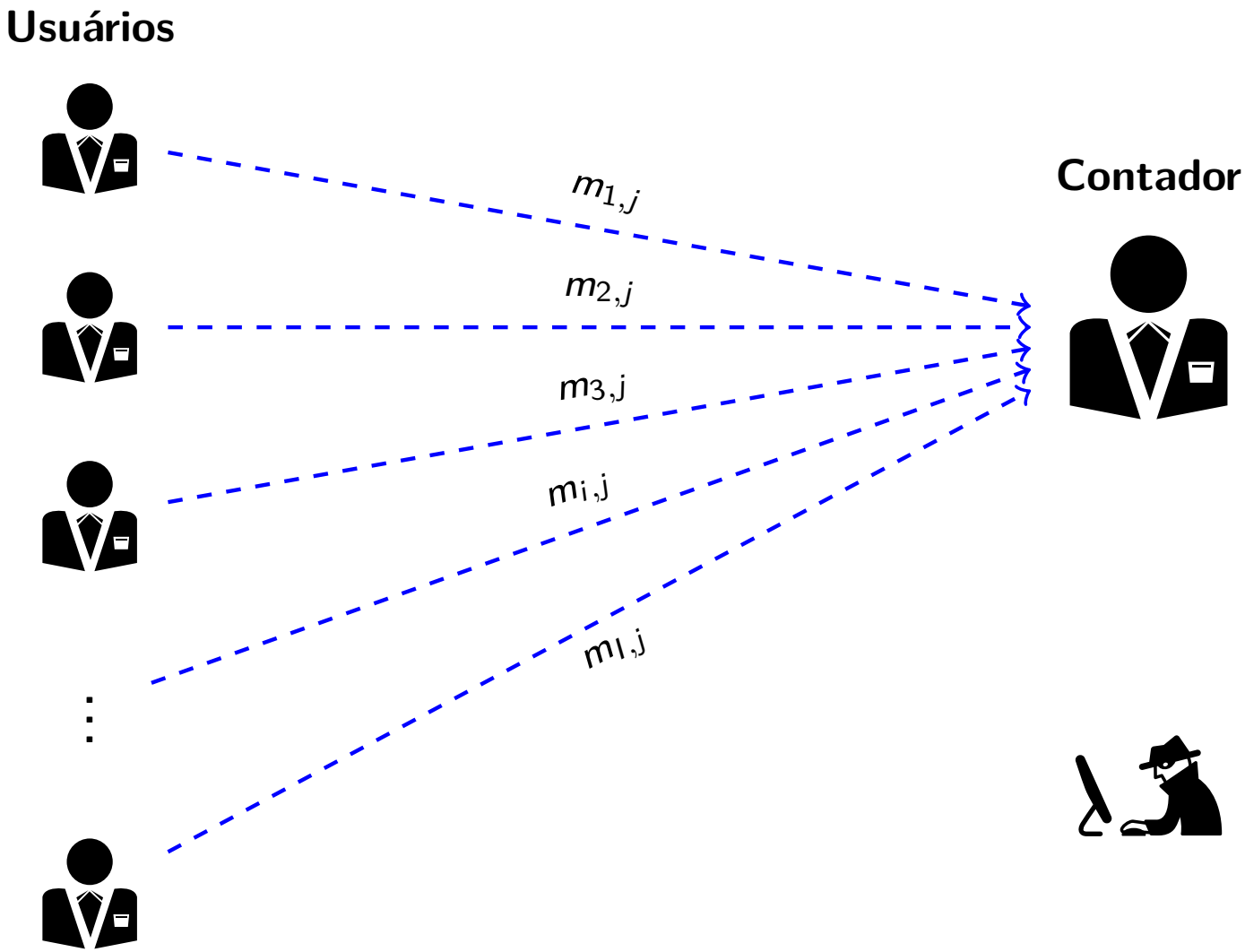




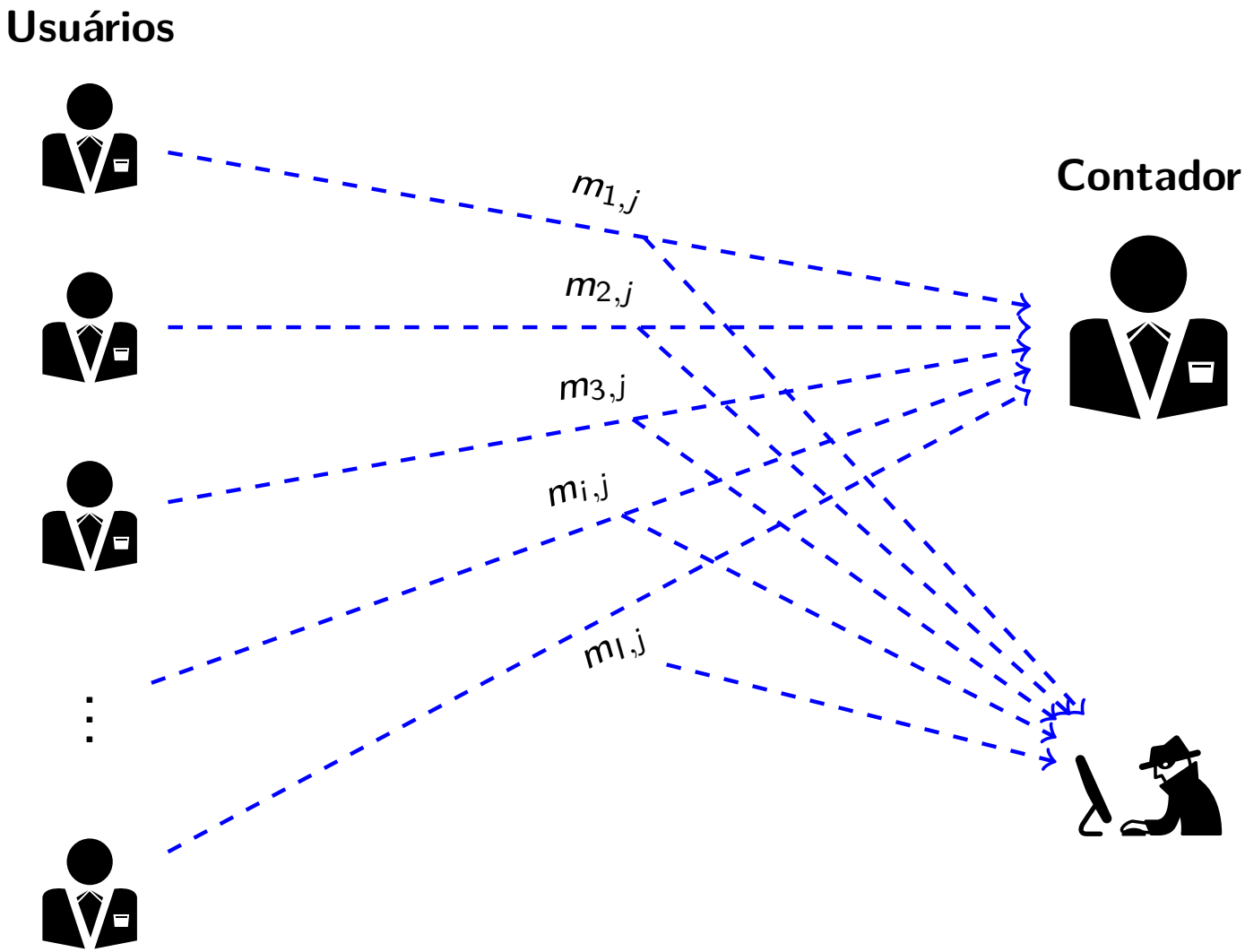
Necessidade de Criptografia



Necessidade de Criptografia

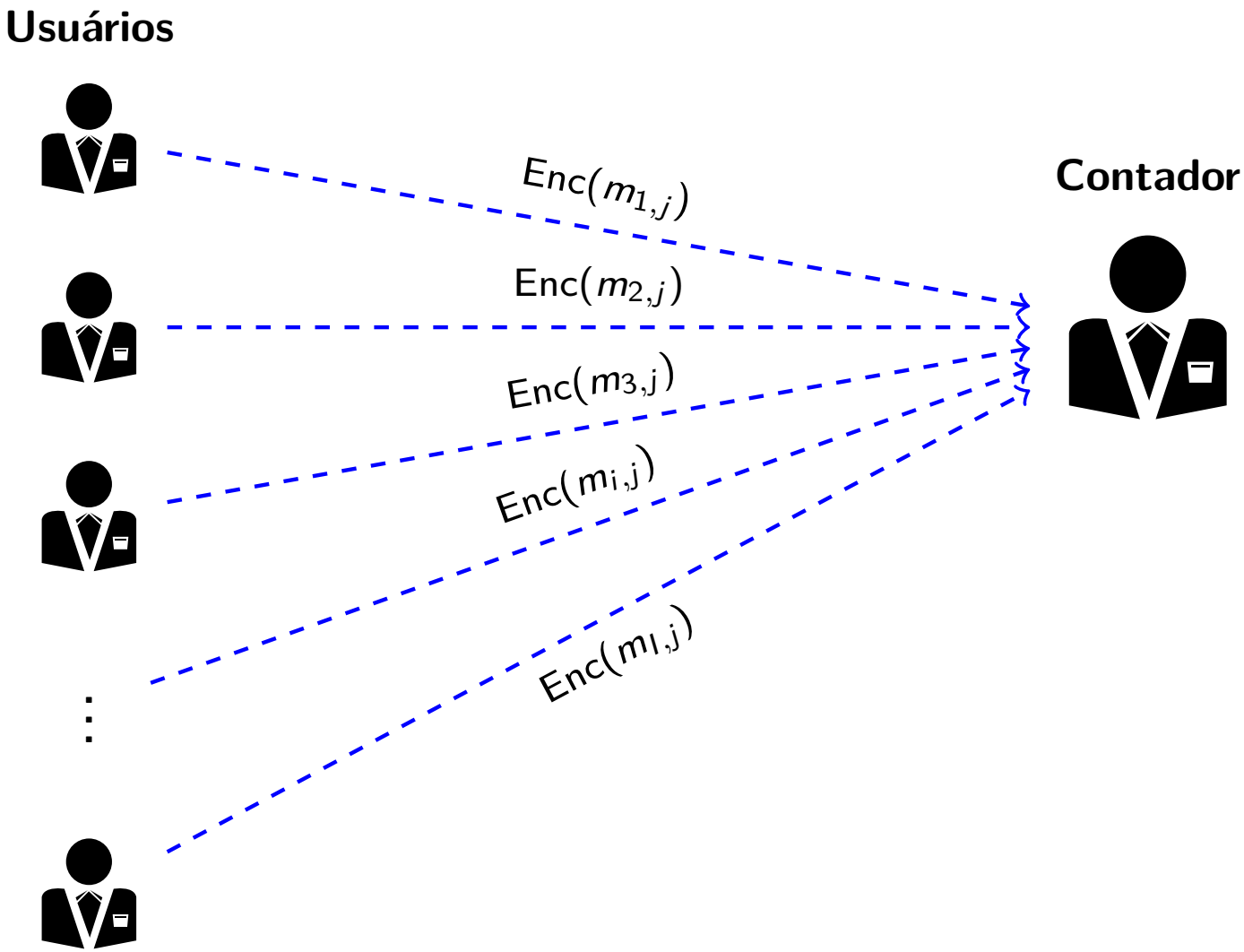


Necessidade de Criptografia



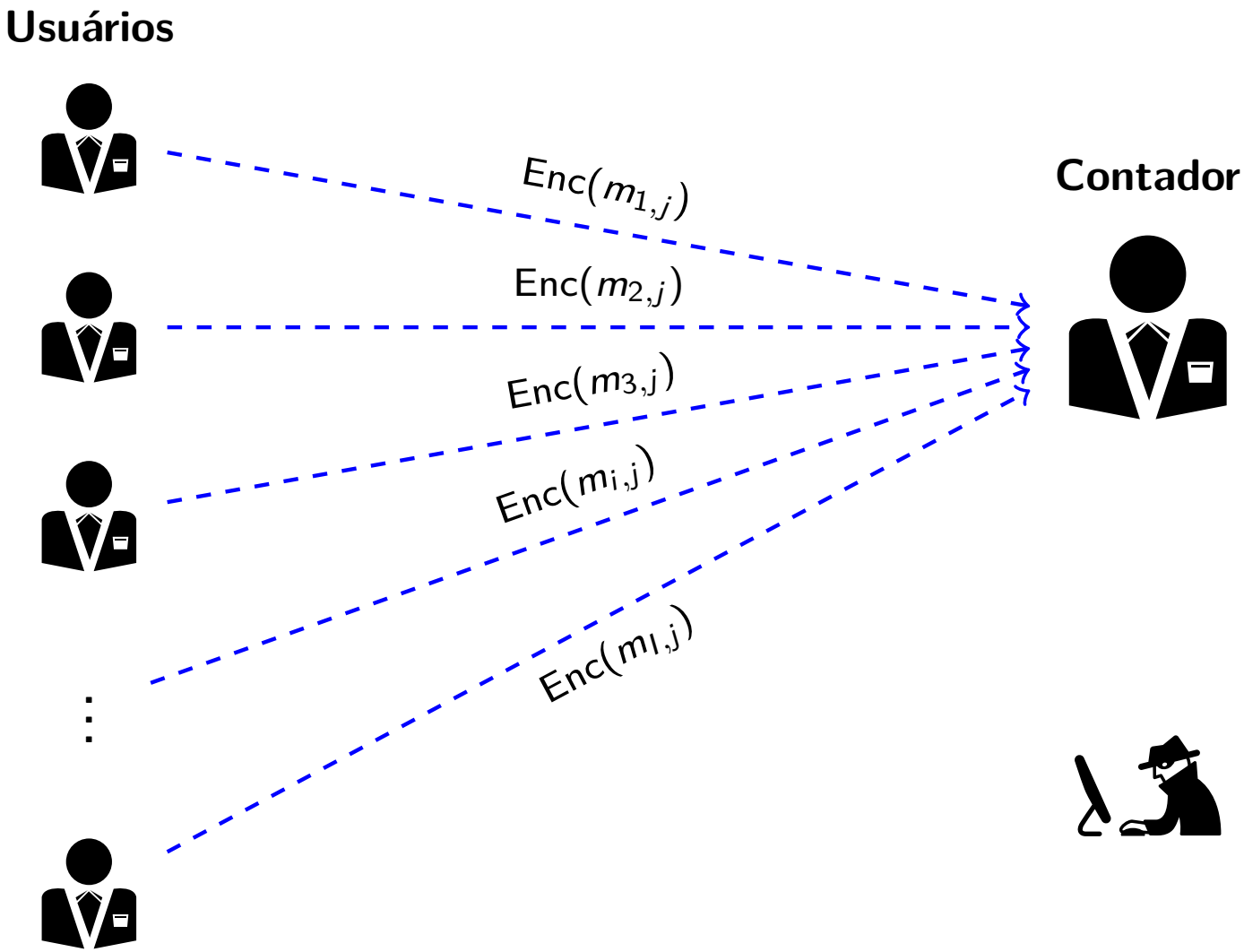
Necessidade de Consolidação

Agregação



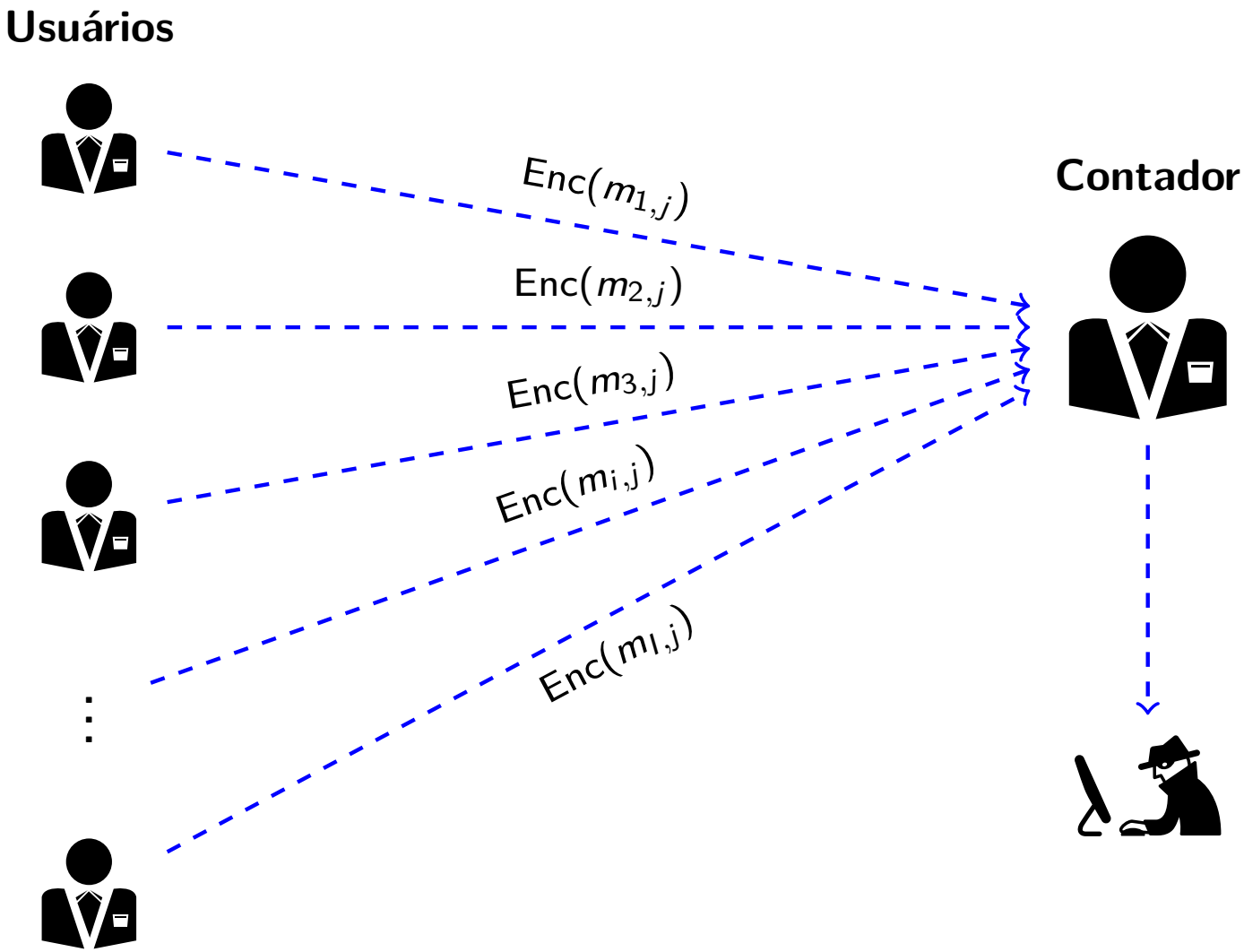
Necessidade de Consolidação

Agregação



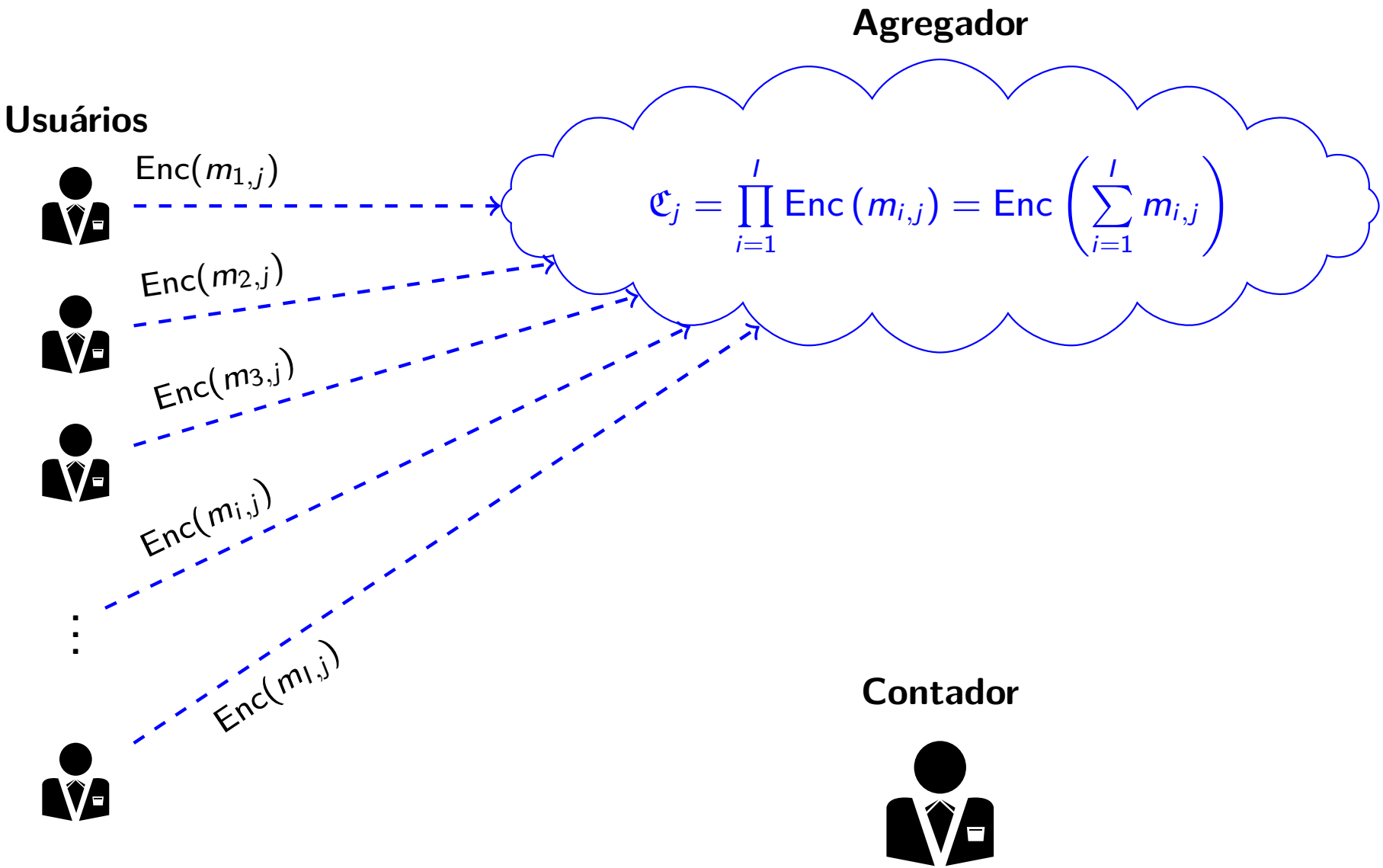
Necessidade de Consolidação

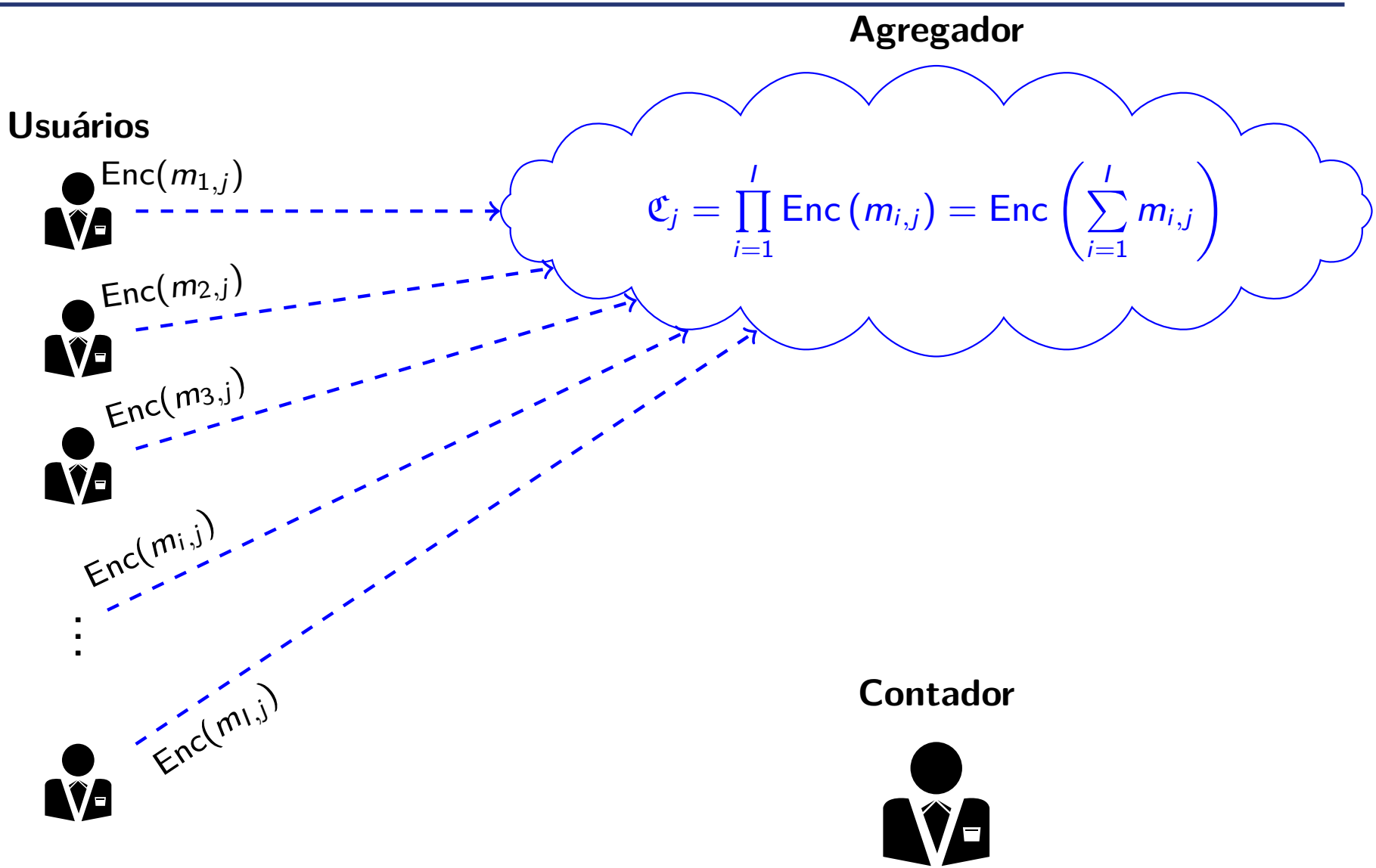
Agregação

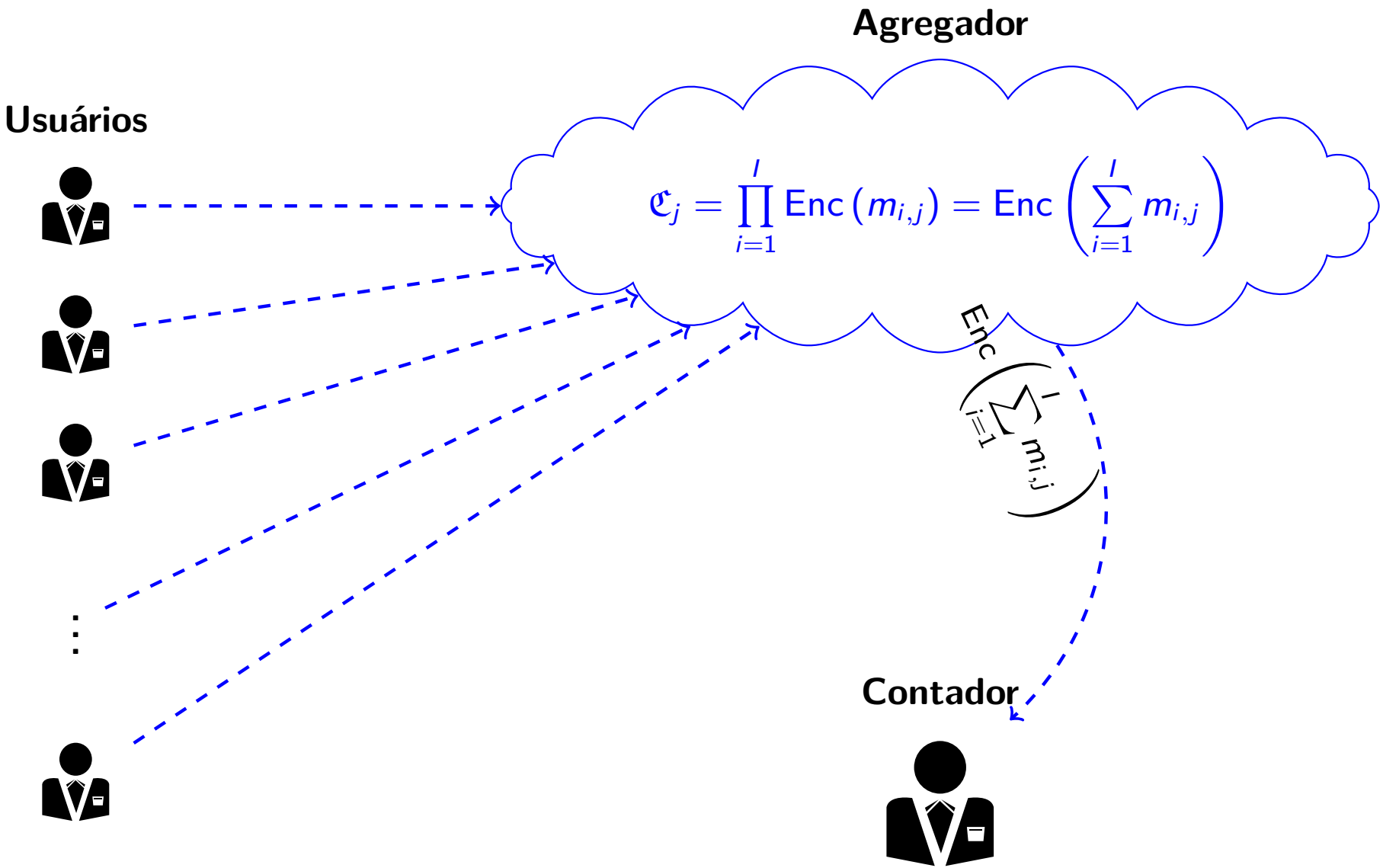


Agregação

Primitiva de criptografia homomórfica aditivas (PCHAs)

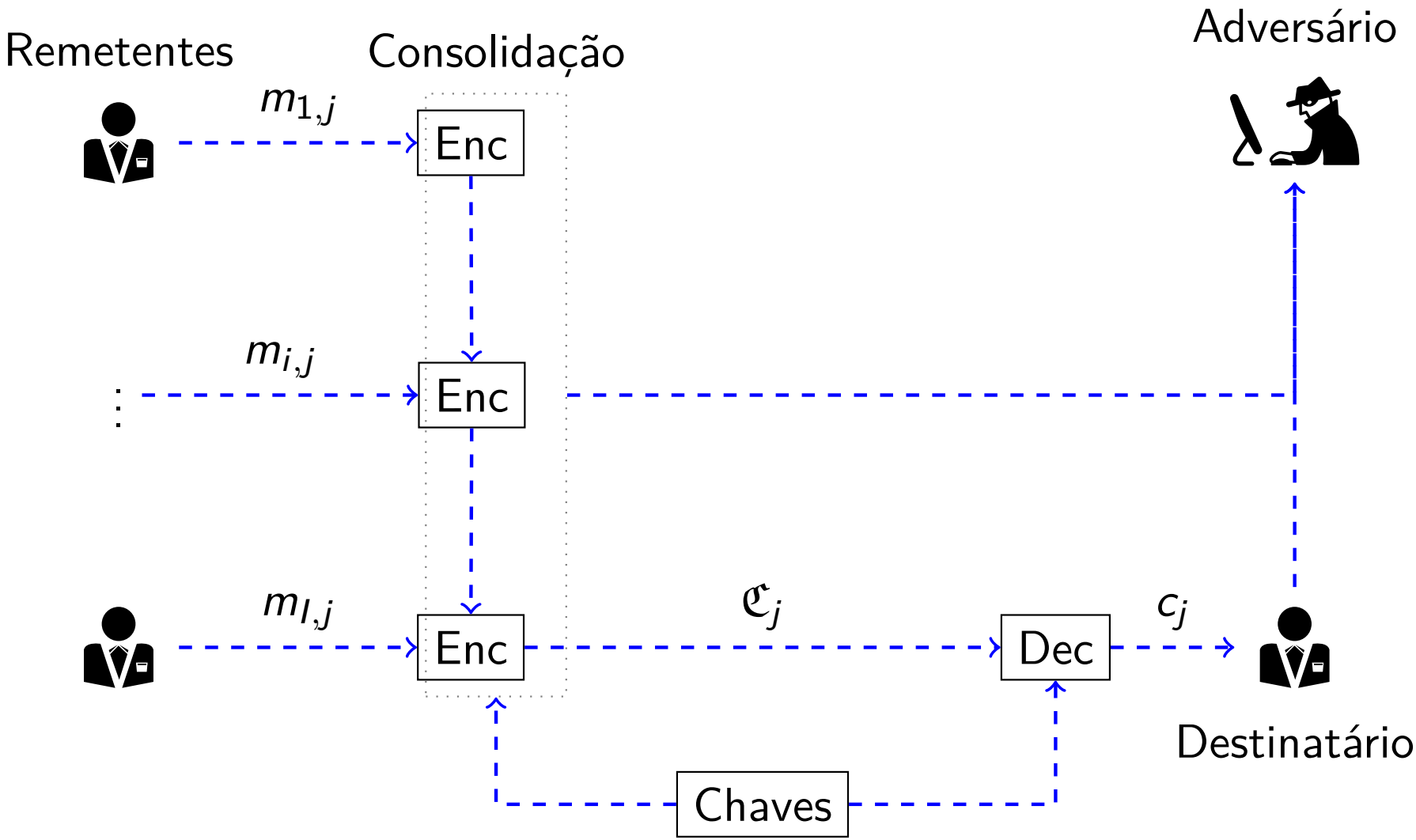


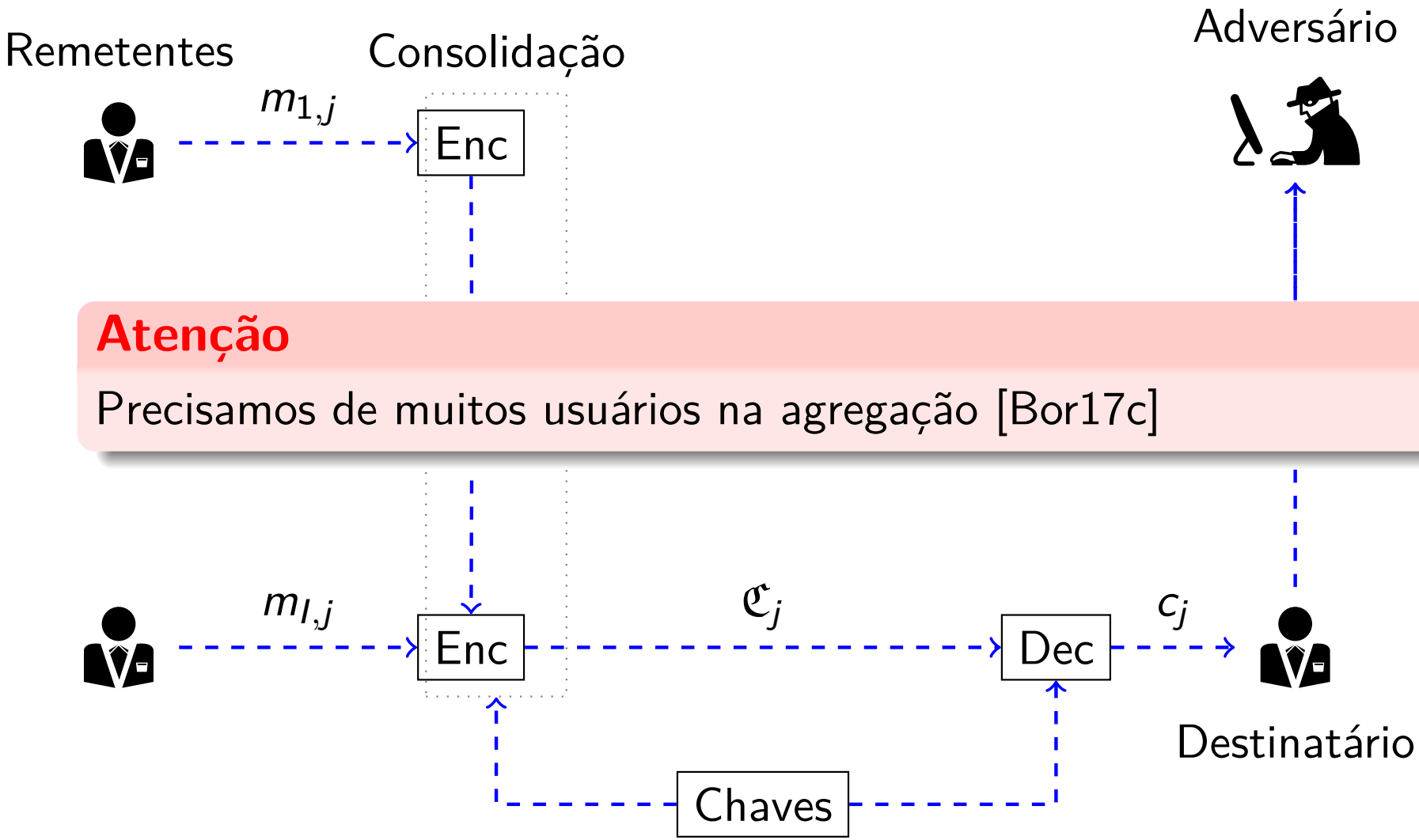

Agregador
Usuários
Enc($m_{1,j}$)
Enc($m_{2,j}$)
Enc($m_{3,j}$)
Enc($m_{i,j}$)
Enc($m_{I,j}$)
$\mathfrak{C}_j = \prod_{i=1}^{I} \mathrm{Enc}(m_{i,j}) = \mathrm{Enc}\left(\sum_{i=1}^{I} m_{i,j}\right)$
Contador


Agregador
Usuários
$\mathfrak{C}_j = \prod_{i=1}^{I} \mathrm{Enc}(m_{i,j}) = \mathrm{Enc}\left(\sum_{i=1}^{I} m_{i,j}\right)$
Enc
$\sum_{i=1}^{I} m_{i,j}$
Contador

Consolidação

Agregação [Bor17a]



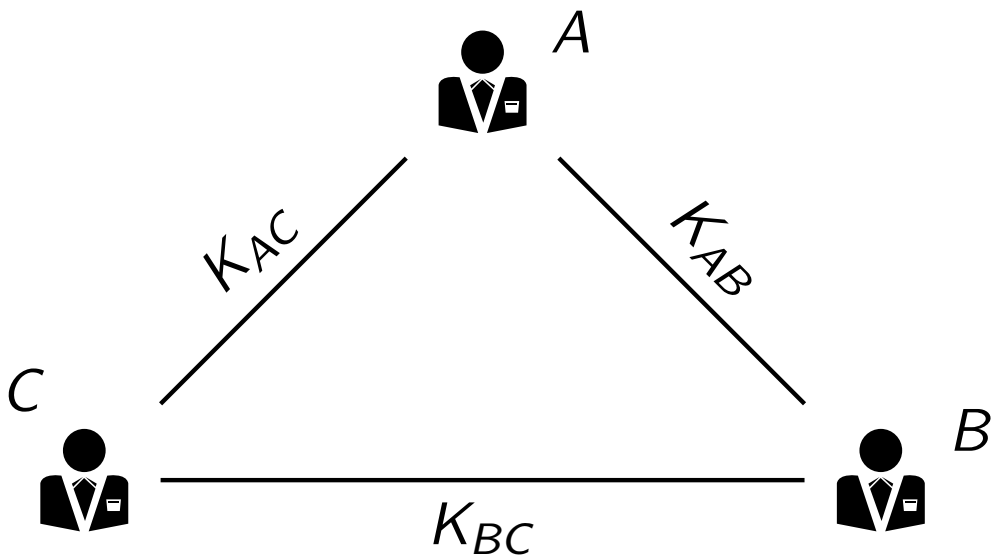


Atenção

Precisamos de muitos usuários na agregação [Bor17c]

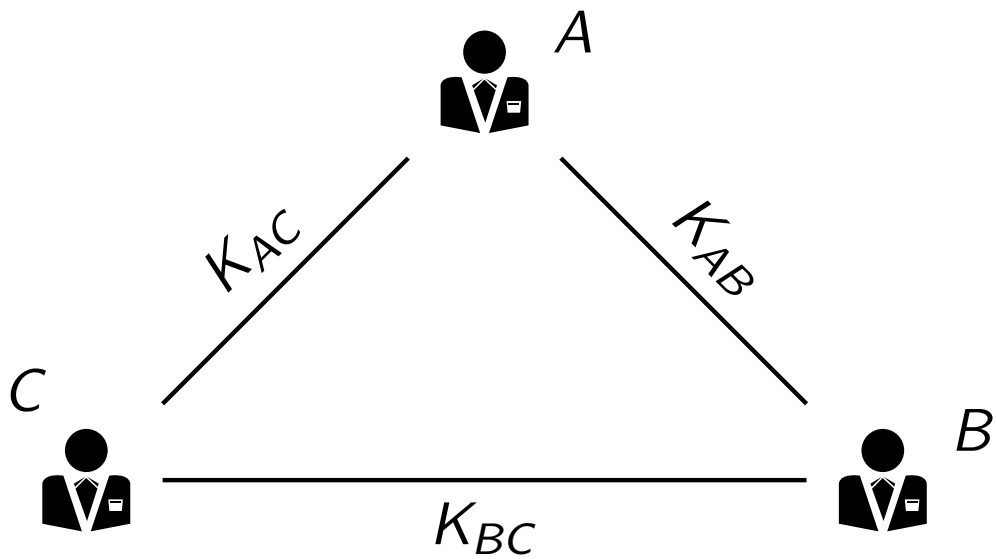
DC-Net simétrica (SDC-Net)

[Cha88] - Dining Cryptographers Problem



SDC-Net

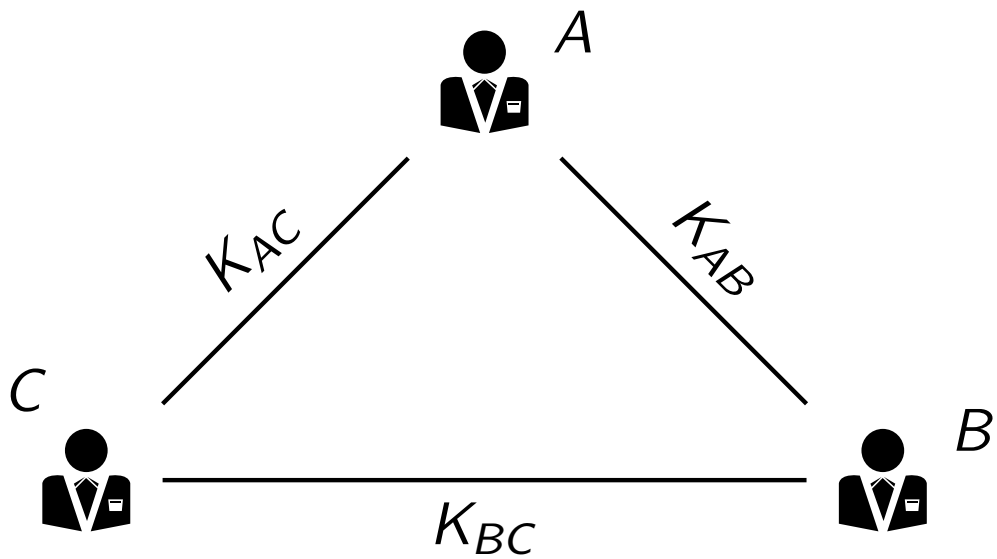
[Cha88] - Dining Cryptographers Problem



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

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

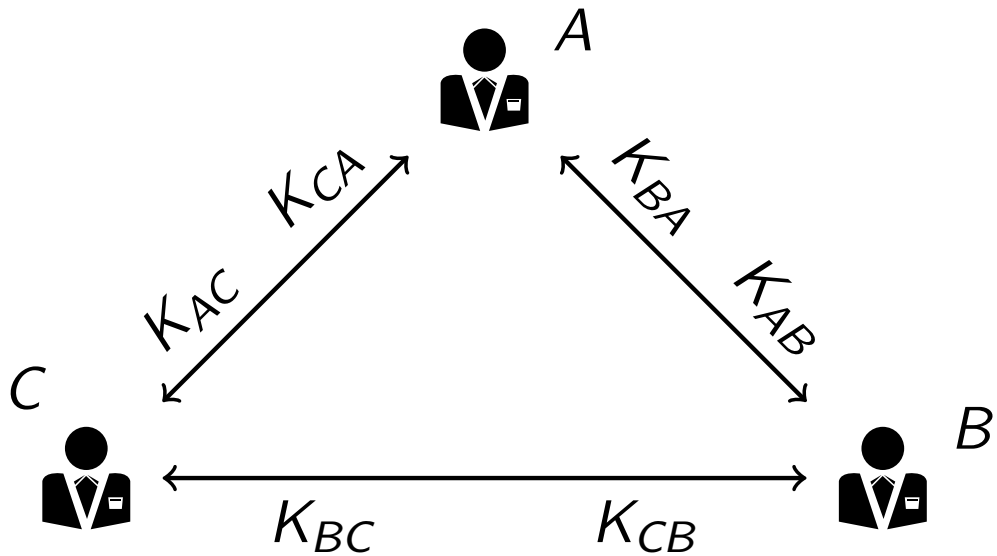
$$K_{Ac} \oplus \underbrace{(K_{AC} \oplus K_{BC})}_{\text{revelado por } C} = K_{BC},$$

ou A teria obtido

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

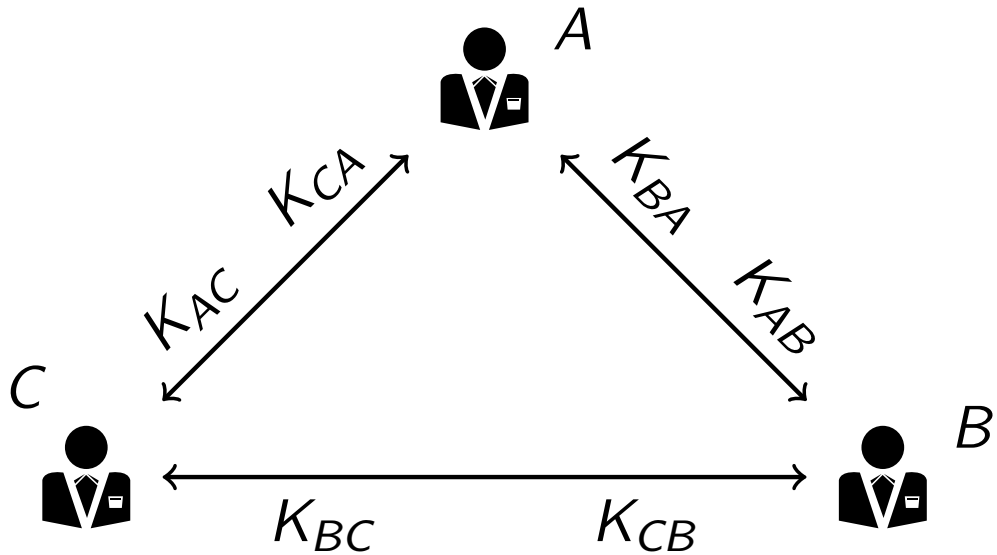
e

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


A
B
C
K_{CA}
K_{AC}
K_{BA}
K_{AB}
K_{BC}
K_{CB}

SDC-Net

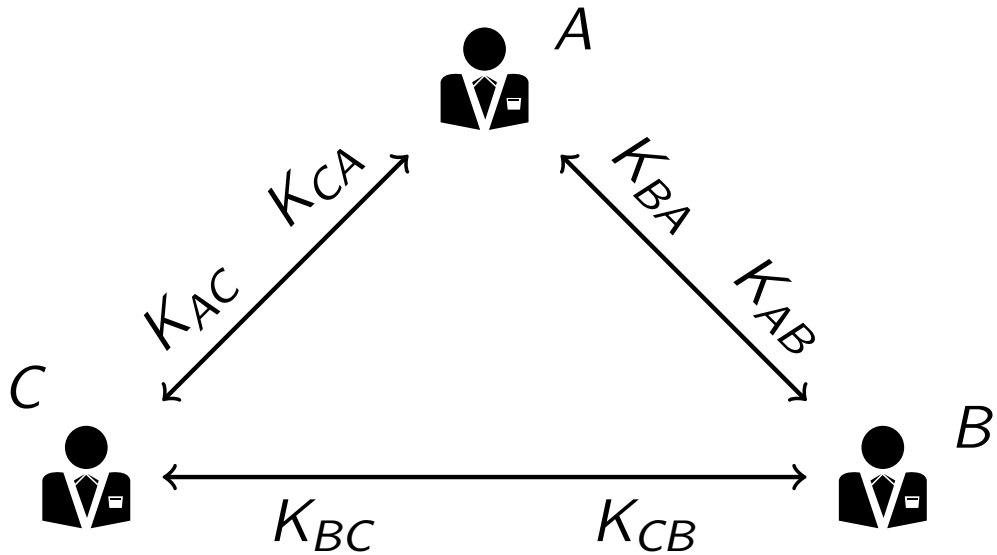
Dígrafo completo



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

SDC-Net

Dígrafo completo



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

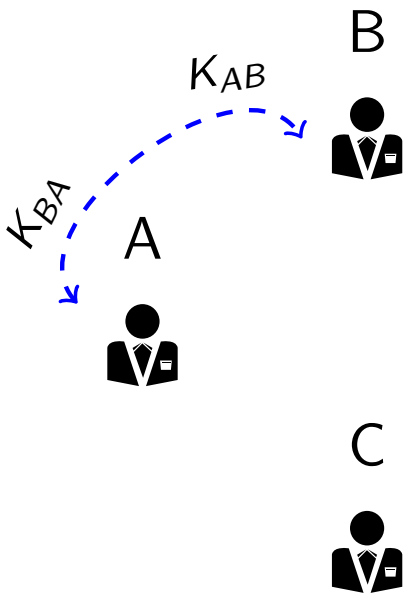
$$c_j = \sum_{i=1}^{I} \mathfrak{M}_{i,j}.$$

SDC-Nets

[Cha88]

SDC-Nets

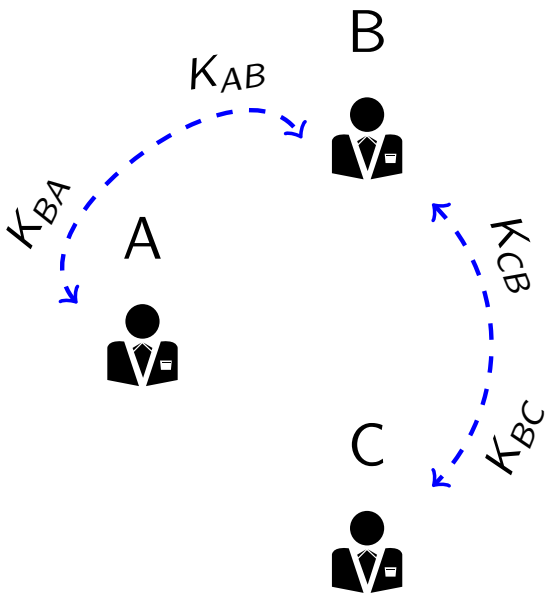
[Cha88]



Contador

SDC-Nets

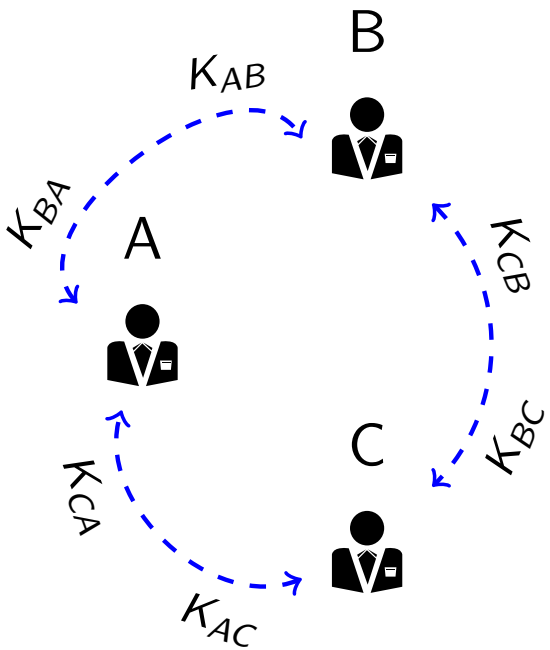
[Cha88]



Contador

SDC-Nets

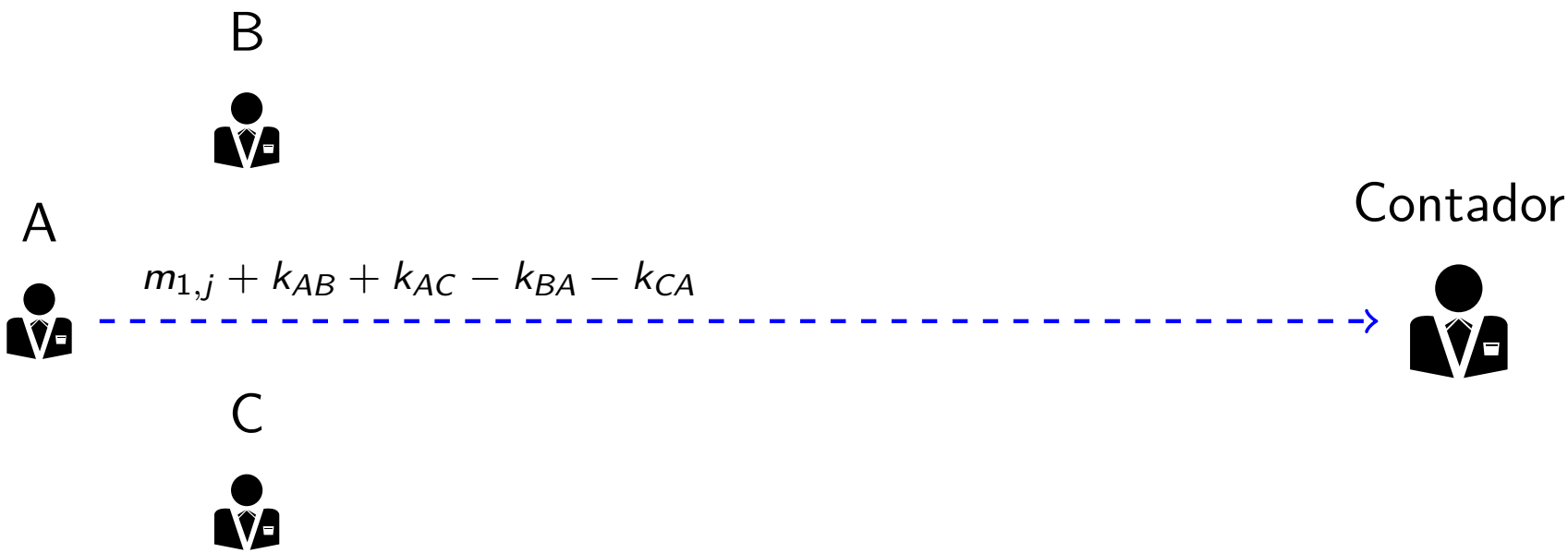
[Cha88]



Contador

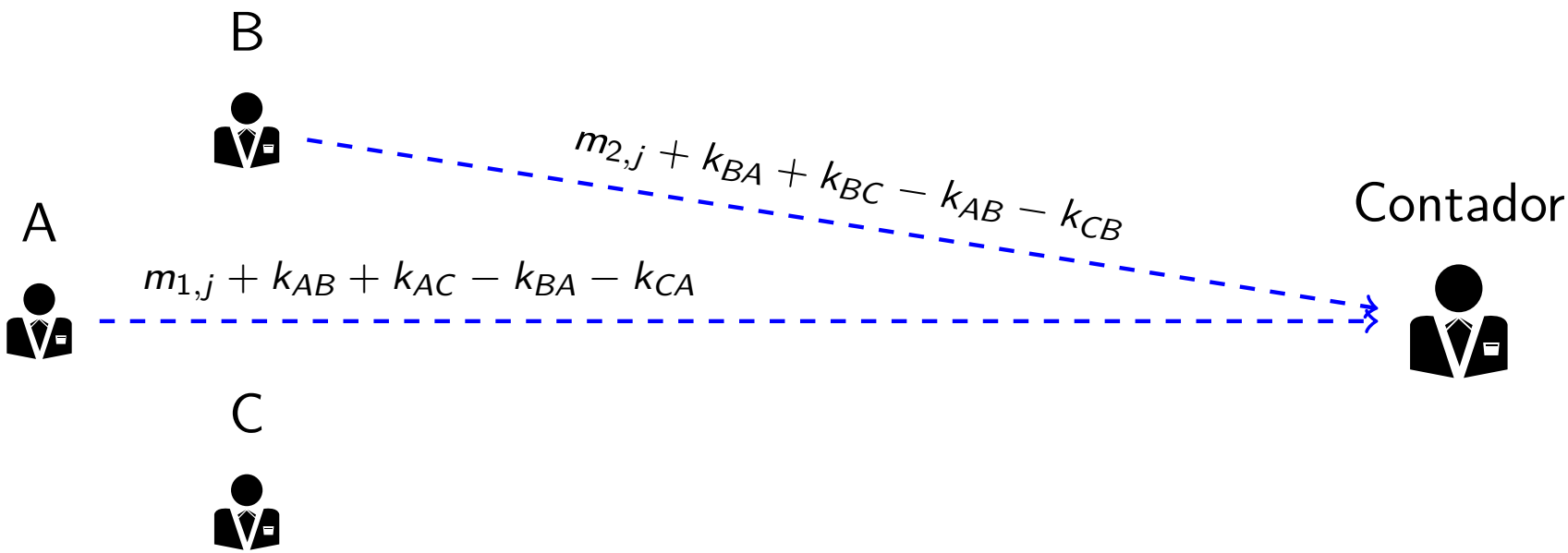
SDC-Nets

Unconditional Secure [Cha88]



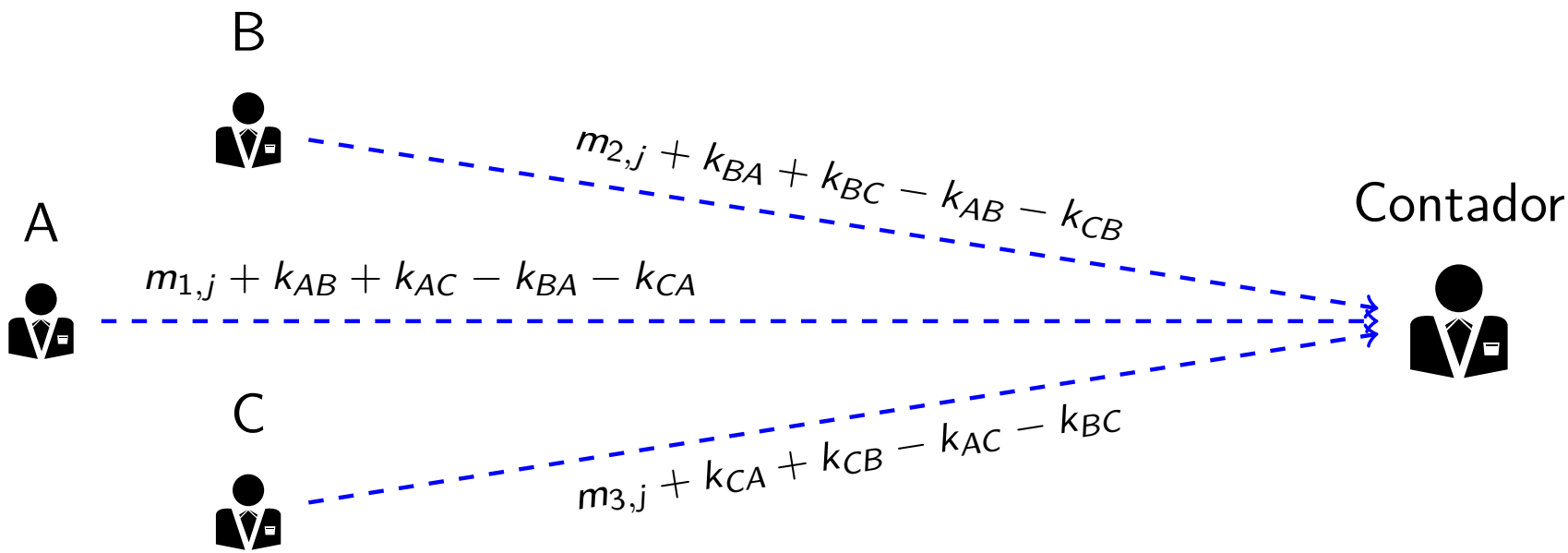
SDC-Nets

Unconditional Secure [Cha88]



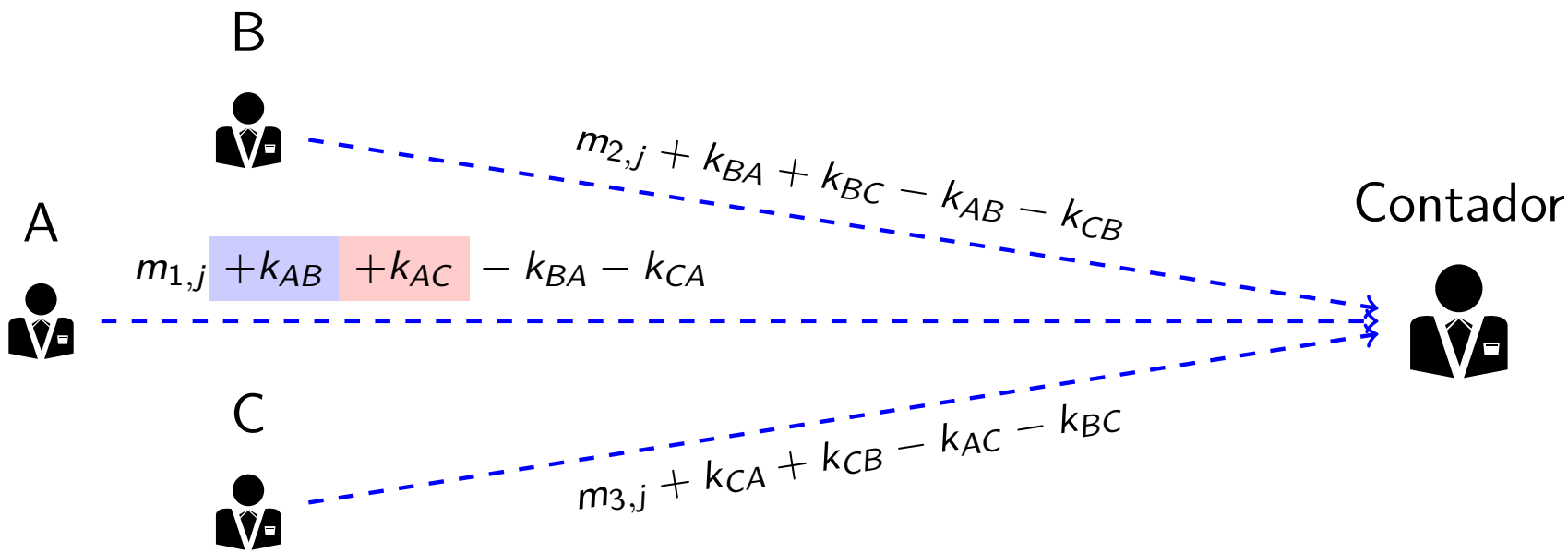
SDC-Nets

Unconditional Secure [Cha88]



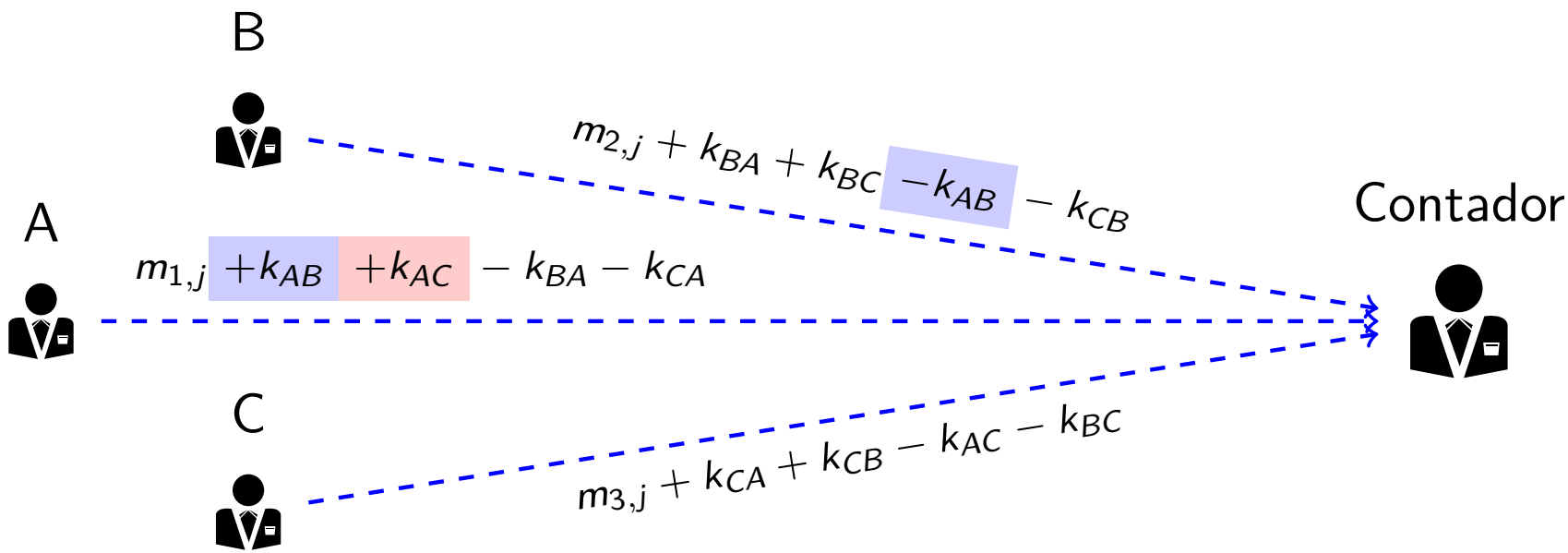
SDC-Nets

Unconditional Secure [Cha88]



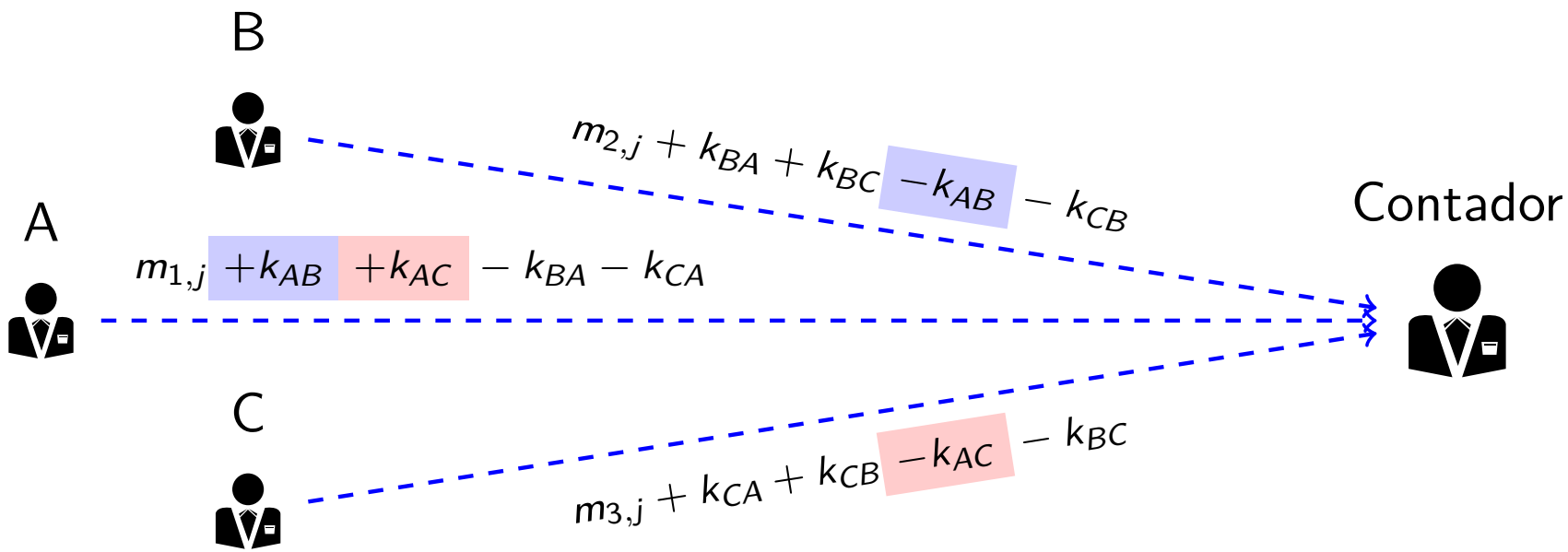
SDC-Nets

Unconditional Secure [Cha88]



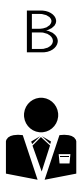
SDC-Nets

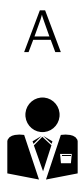
Unconditional Secure [Cha88]



SDC-Nets

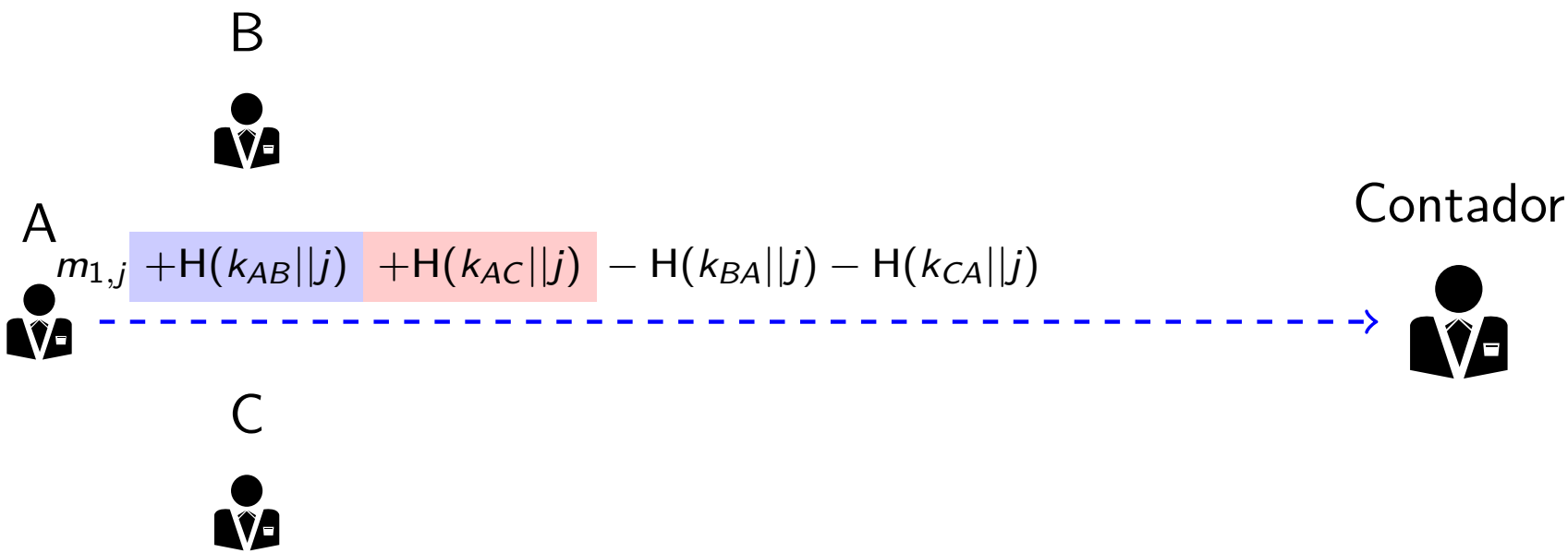
[GJ04]





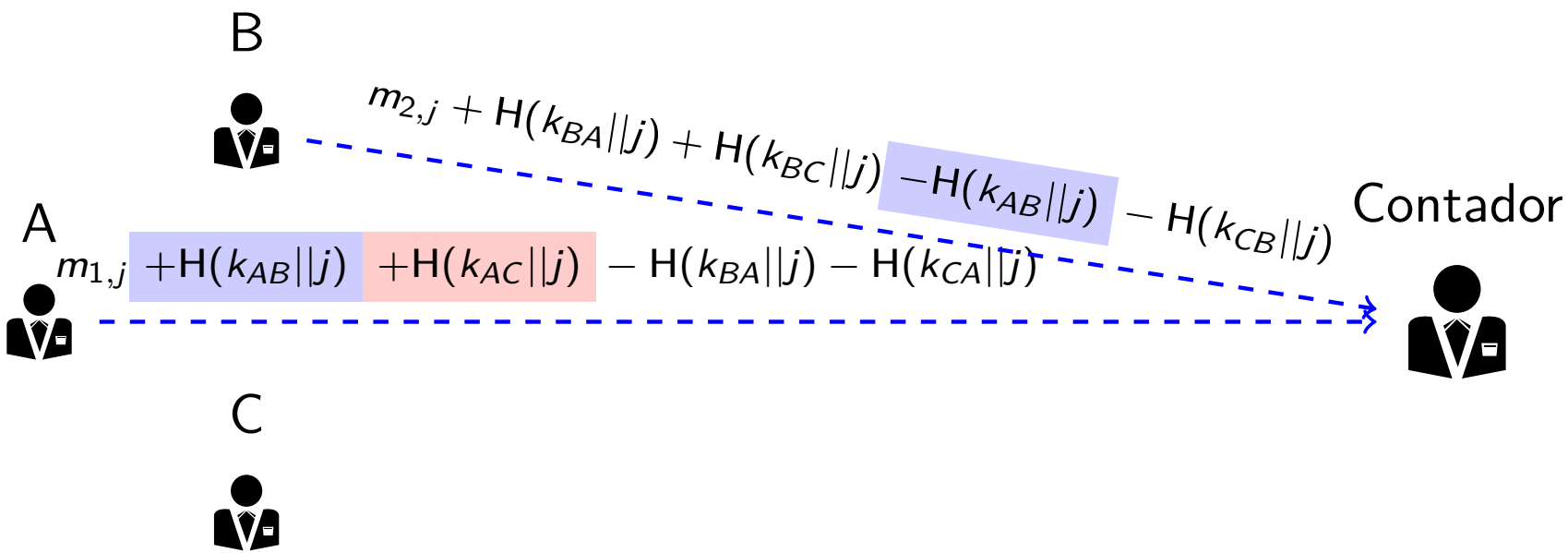
SDC-Nets

[GJ04]



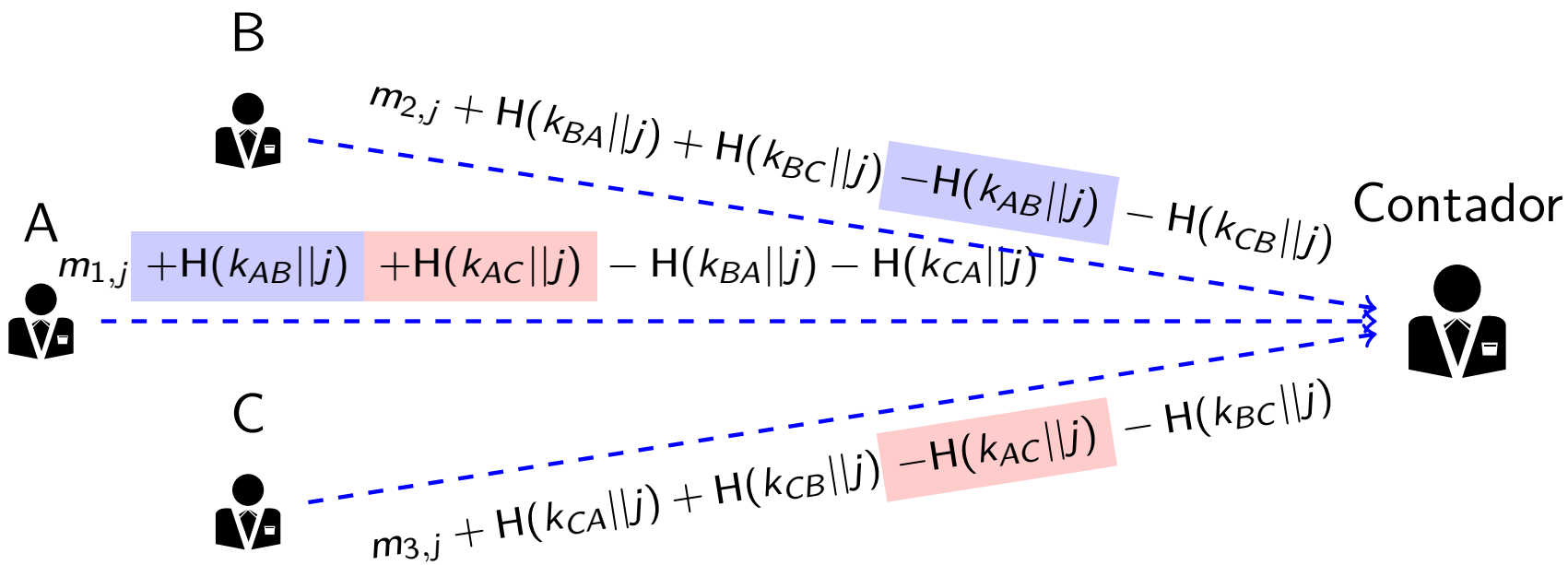
SDC-Nets

[GJ04]



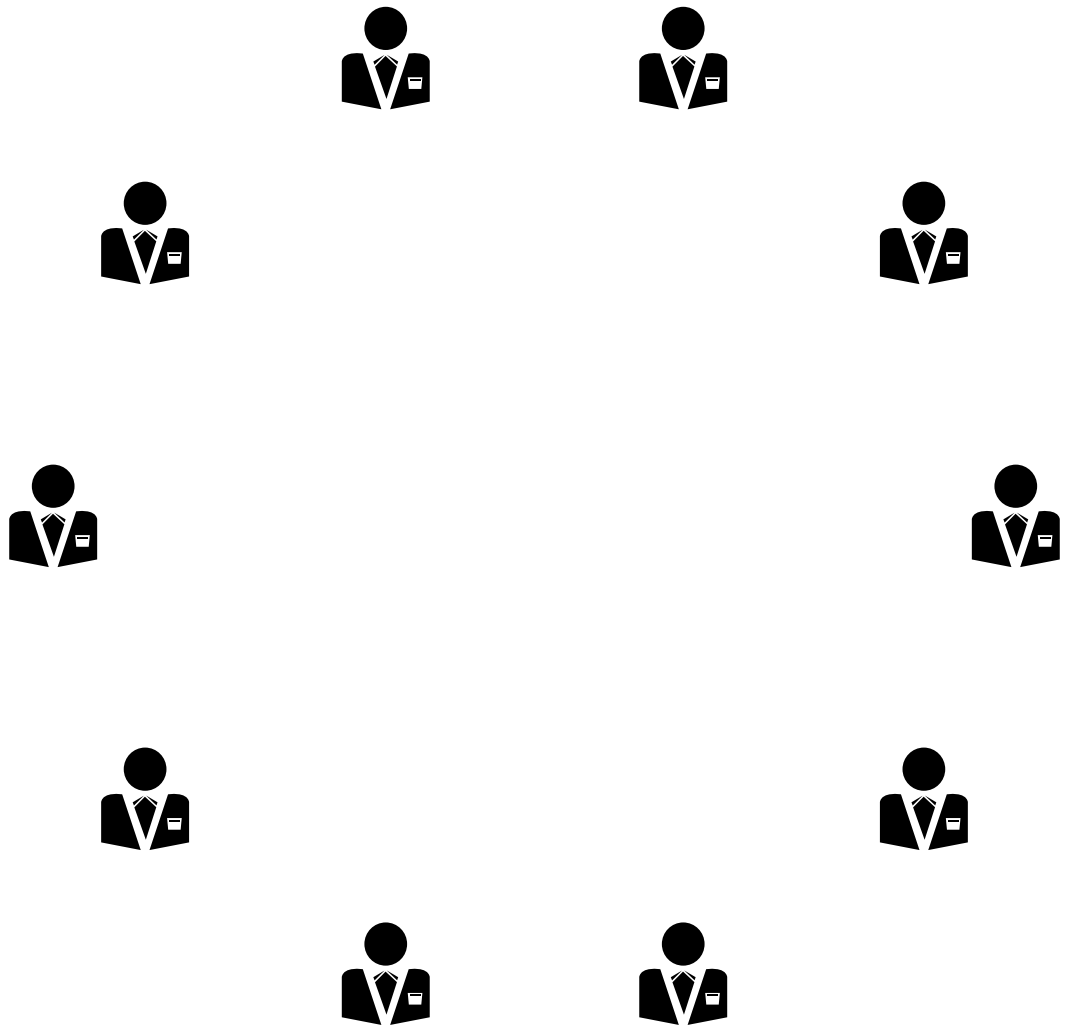
SDC-Nets

[GJ04]



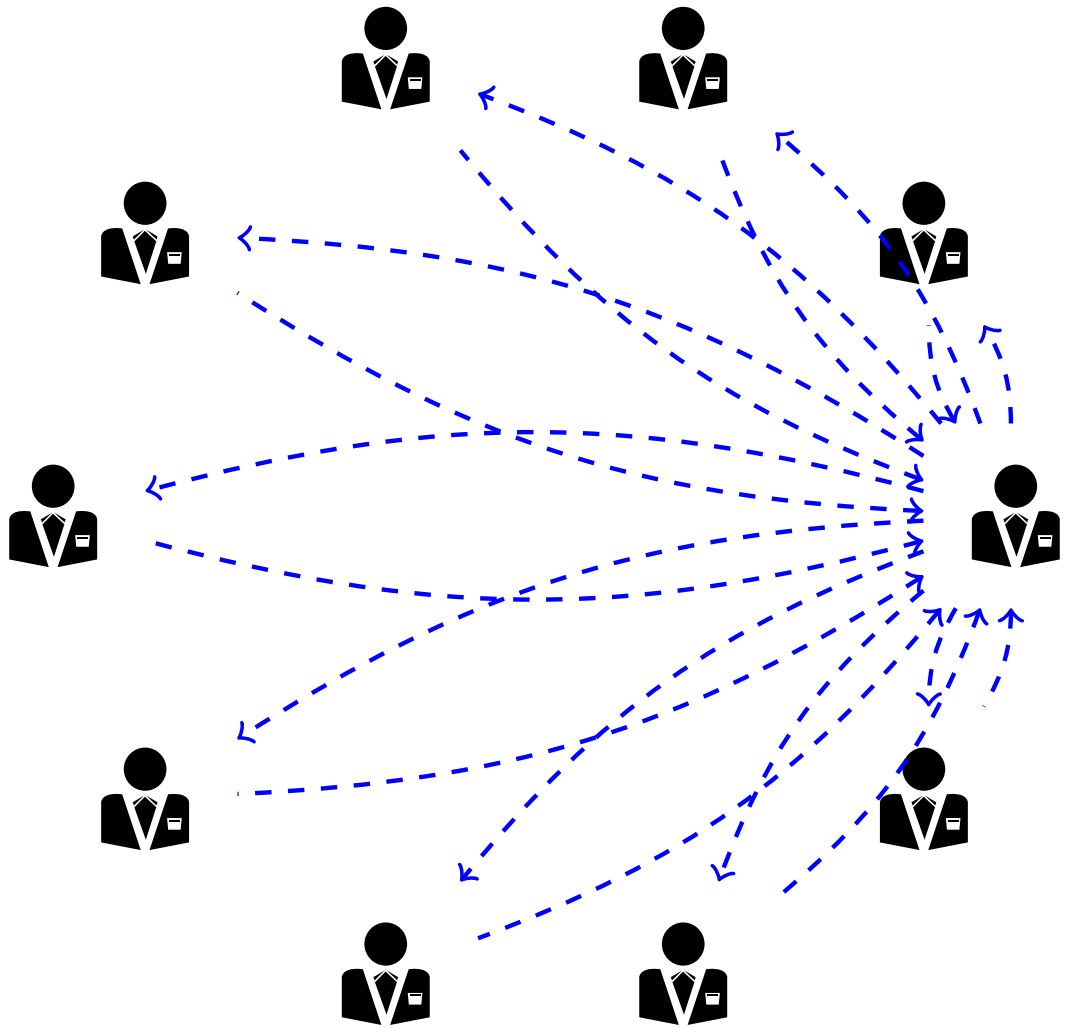
SDC-Net

Chaves para 10 usuários



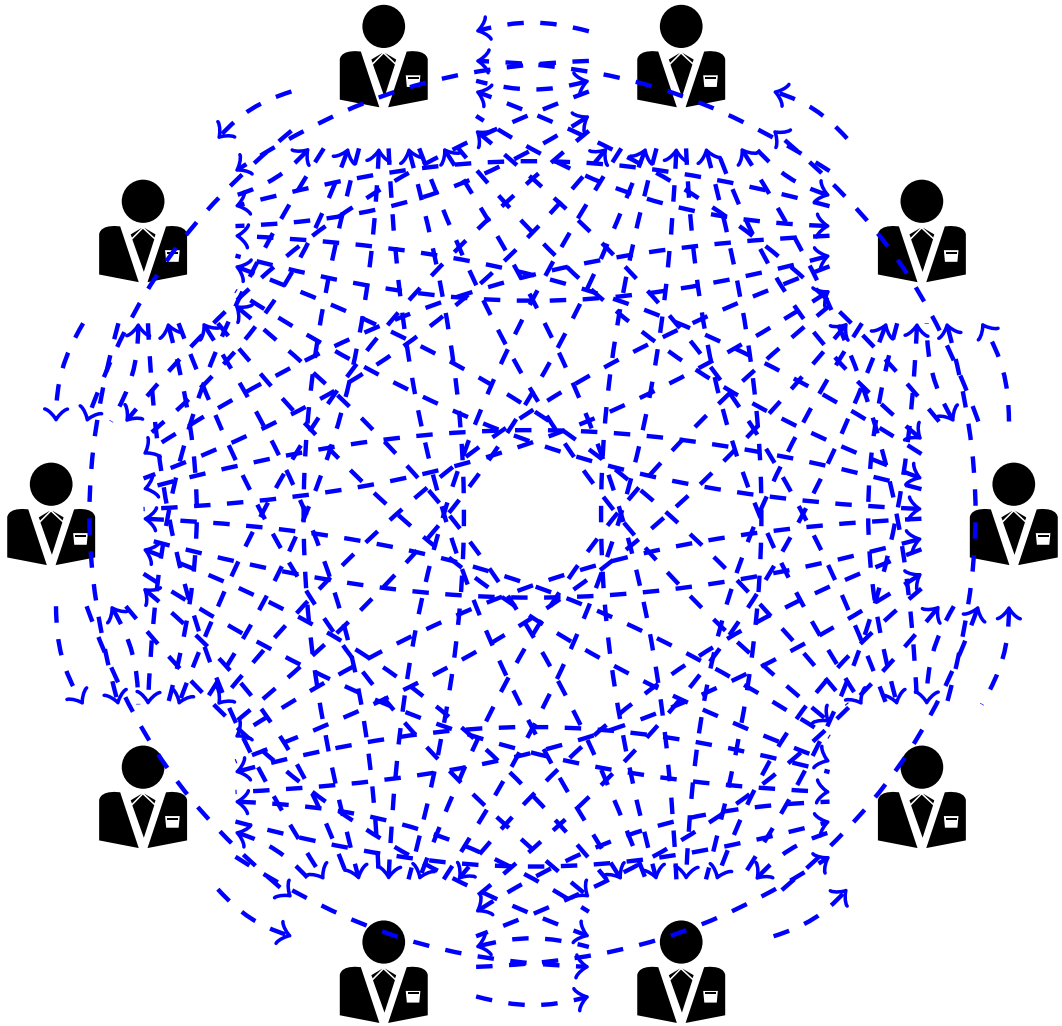
SDC-Net

Chaves para 10 usuários



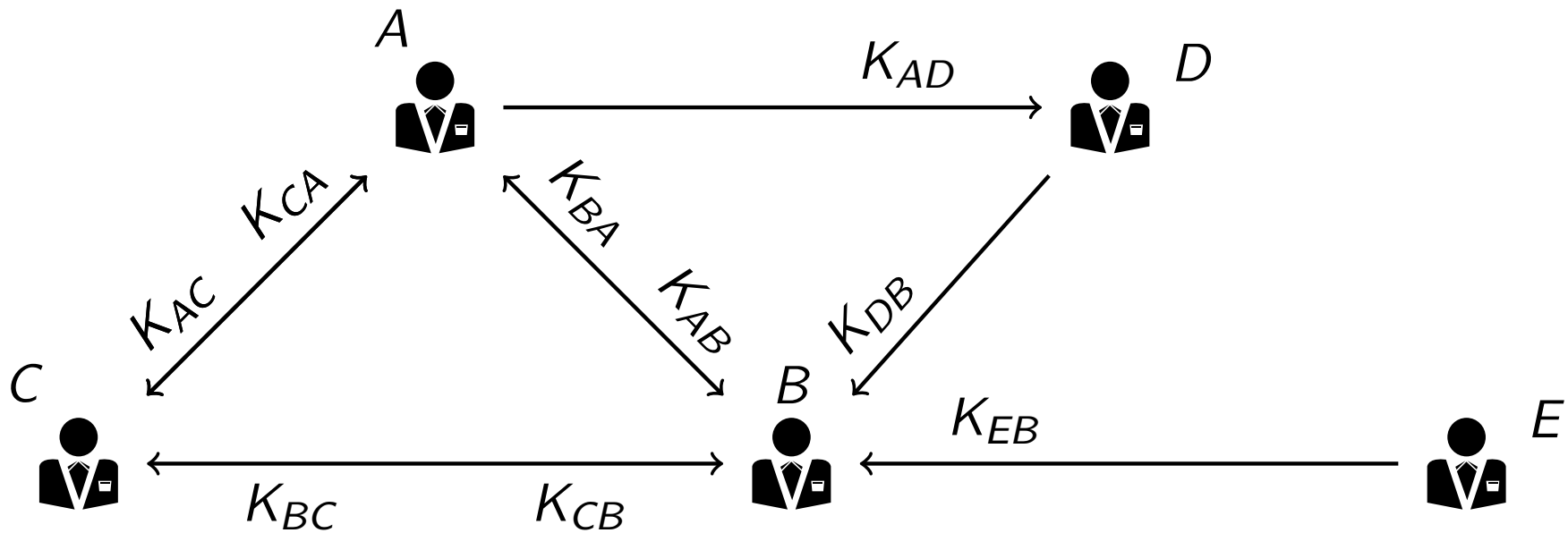
SDC-Net

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

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

DC-Net assimétrica (ADC-Net)

[Bor17d]

Satisfaz as seguintes propriedades:

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

ADC-Net

[Bor17d]

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

[Bor17d]

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

[Bor17d]

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

[Bor17d]

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

[Bor17d]

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;
6. usuários podem mandar o número mínimo de mensagens;

ADC-Net

[Bor17d]

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

[Bor17d]

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

[Bor17d]

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

[Bor17d]

Criptografar

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

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

ADC-Net

[Bor17d]

Criptografar

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

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

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

[Bor17d]

Criptografar

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

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

Descriptografar

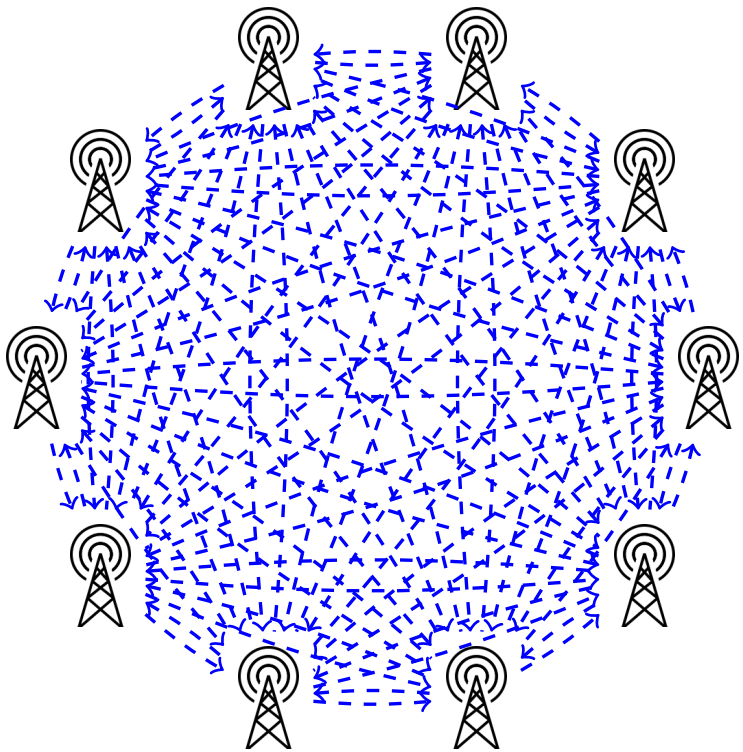
$$\text{Dec} : \mathbb{Z}_{n^2} \to \mathbb{Z}_n$$

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

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

Configurando as chaves

DC-Nets versus criptografia homomórfica



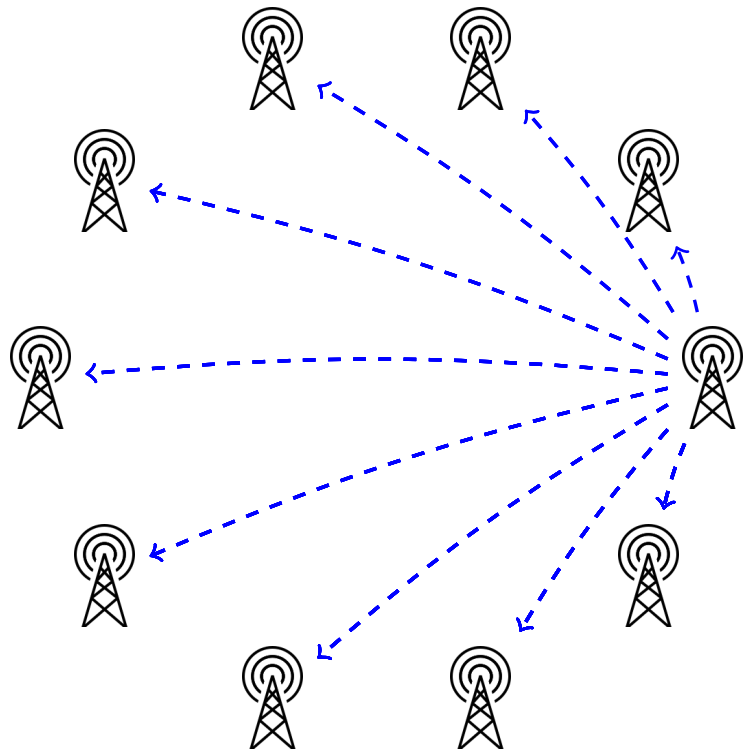


Table of Contents

Perspectivas

Segurança & Privacidade

Computação Ubíqua é “a ideia de integrar computadores perfeitamente no mundo em geral" [Wei91].

Perspectivas

Segurança & Privacidade

Computação Ubíqua é “a ideia de integrar computadores perfeitamente no mundo em geral" [Wei91].

Frequentemente:

1. Software UbiComp é produzido com várias linguagens de tipo inseguras.

Perspectivas

Segurança & Privacidade

Computação Ubíqua é “a ideia de integrar computadores perfeitamente no mundo em geral" [Wei91].

Frequentemente:

1. Software UbiComp é produzido com várias linguagens de tipo inseguras.
2. O acesso físico e os recursos restritos levam a ataques de canais laterais.

Perspectivas

Segurança & Privacidade

Computação Ubíqua é “a ideia de integrar computadores perfeitamente no mundo em geral" [Wei91].

Frequentemente:

1. Software UbiComp é produzido com várias linguagens de tipo inseguras.
2. O acesso físico e os recursos restritos levam a ataques de canais laterais.
3. Grandes volumes de dados complicam a proteção da privacidade dos usuários.

Perspectivas

Segurança & Privacidade

Computação Ubíqua é “a ideia de integrar computadores perfeitamente no mundo em geral" [Wei91].

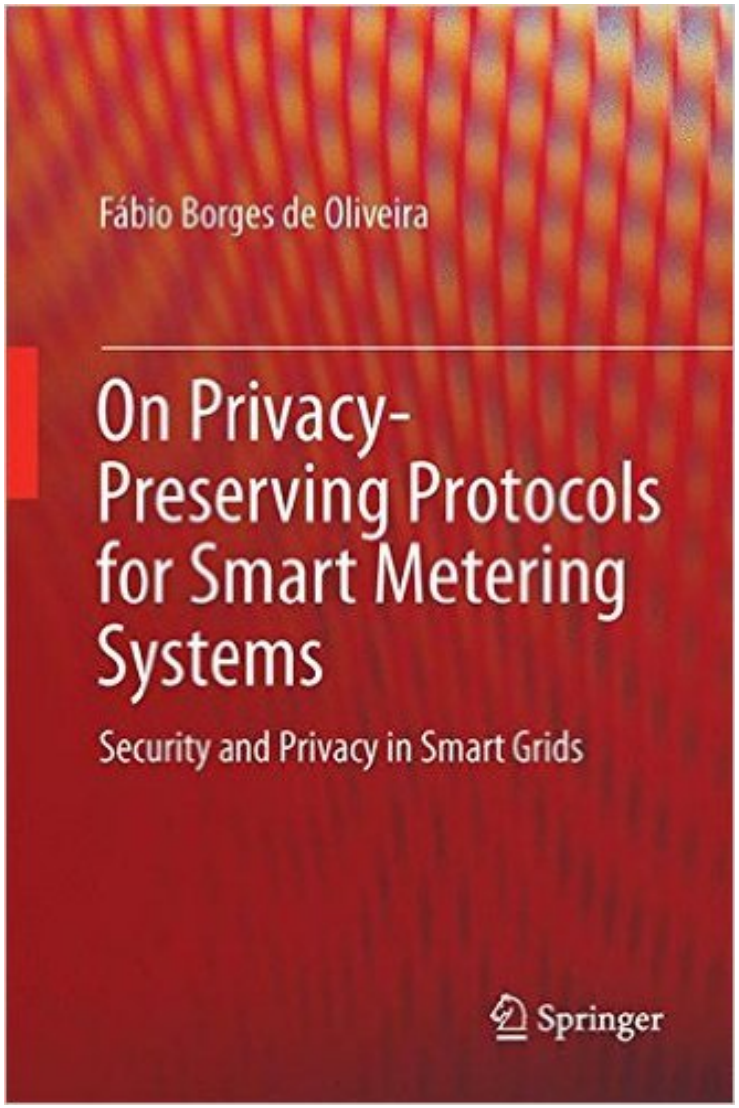
Frequentemente:

1. Software UbiComp é produzido com várias linguagens de tipo inseguras.
2. O acesso físico e os recursos restritos levam a ataques de canais laterais.
3. Grandes volumes de dados complicam a proteção da privacidade dos usuários.
4. Novas tecnologias são ameaças para segurança a longo prazo.

Book

[Bor17b]

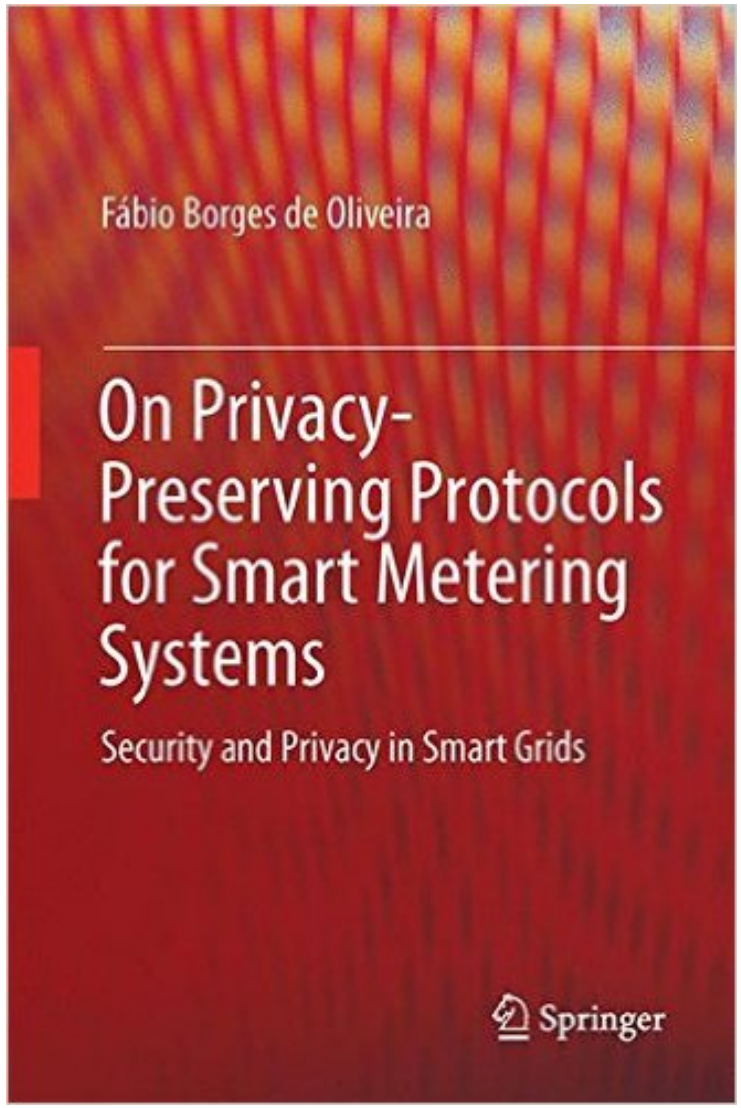
- Ubiquitous computing (ubicomp)



Book

[Bor17b]

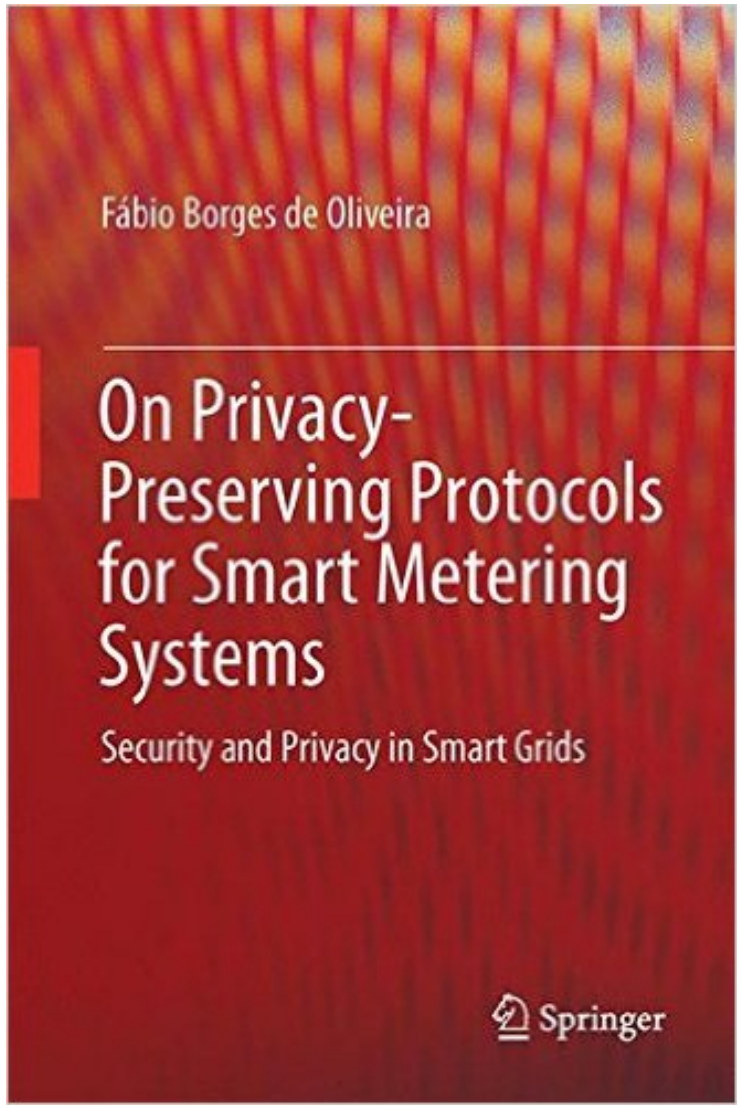
- Ubiquitous computing (ubicomp)
- Cyber-physical system



Book

[Bor17b]

- Ubiquitous computing (ubicomp)
- Cyber-physical system
- Internet of Thinks (IoT)



Thank You!

All comments and suggestions are welcomed.
Contact:

borges@lncc.br
www.lncc.br/∼borges/

Fábio Borges de Oliveira

Bibliografia I

Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: a survey. *Computer Networks*, 54(15):2787–2805, 2010.

Kevin Ashton. That 'Internet of Things' Thing. *RFiD Journal*, 22:97–114, 2009.

Fábio Borges de Oliveira. *Background and models*. In *On Privacy-Preserving Protocols for Smart Metering Systems: Security and Privacy in Smart Grids*. Springer International Publishing, Cham, 2017, pages 13–23.

Fábio Borges de Oliveira. *On Privacy-Preserving Protocols for Smart Metering Systems: Security and Privacy in Smart Grids*. Springer International Publishing, Cham, 2017.

Fábio Borges de Oliveira. *Quantifying the aggregation size*. In *On Privacy-Preserving Protocols for Smart Metering Systems: Security and Privacy in Smart Grids*. Springer International Publishing, Cham, 2017, pages 49–60.

Bibliografia II

Fábio Borges de Oliveira. *Selected privacy-preserving protocols*. In *On Privacy-Preserving Protocols for Smart Metering Systems: Security and Privacy in Smart Grids*. Springer International Publishing, Cham, 2017, pages 61–100.

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

Deborah Estrin, Ramesh Govindan, John S. Heidemann, and Satish Kumar. Next century challenges: scalable coordination in sensor networks. In *MobiCom'99*, pages 263–270, 1999.

Philippe Golle and Ari Juels. *Dining cryptographers revisited*. In *Advances in Cryptology - EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings*. Christian Cachin and Jan L. Camenisch, editors. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pages 456–473.

Bibliografia III

Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of ACM STOC 1996*, pages 212–219, Philadelphia, Pennsylvania, USA. ACM, 1996.

Edward A Lee. Cyber-physical systems-are computing foundations adequate. In *NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, volume 2. Citeseer, 2006.

N. Li, T. Li, and S. Venkatasubramanian. T-closeness: privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering*, pages 106–115, April 2007.

Kalle Lyytinen and Youngjin Yoo. Ubiquitous computing. *Communications of the ACM*, 45(12):63–96, 2002.

Steve Mann. Wearable computing: a first step toward personal imaging. *Computer*, 30(2):25–32, 1997.

Tom Martin and Jennifer Healey. 2006's wearable computing advances and fashions. *IEEE Pervasive Computing*, 6(1), 2007.

Bibliografia IV

M. Nogueira. *SAMNAR: A survivable architecture for wireless self-organizing networks*. PhD thesis, Université Pierre et Marie Curie - LIP6, 2009.

G. J. Pottie and W. J. Kaiser. Wireless Integrated Network Sensors. *Communications ACM*, 43(5):51–58, 2000.

Ragunathan Raj Rajkumar, Insup Lee, Lui Sha, and John Stankovic. Cyber-physical systems: the next computing revolution. In *47th Design Automation Conference*. ACM, 2010.

Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

Mark Weiser. The computer for the 21st century. *Scientific american*, 265(3):94–104, 1991.

Mark Weiser. Some computer science issues in ubiquitous computing. *Communications of the ACM*, 36(7):75–84, 1993.