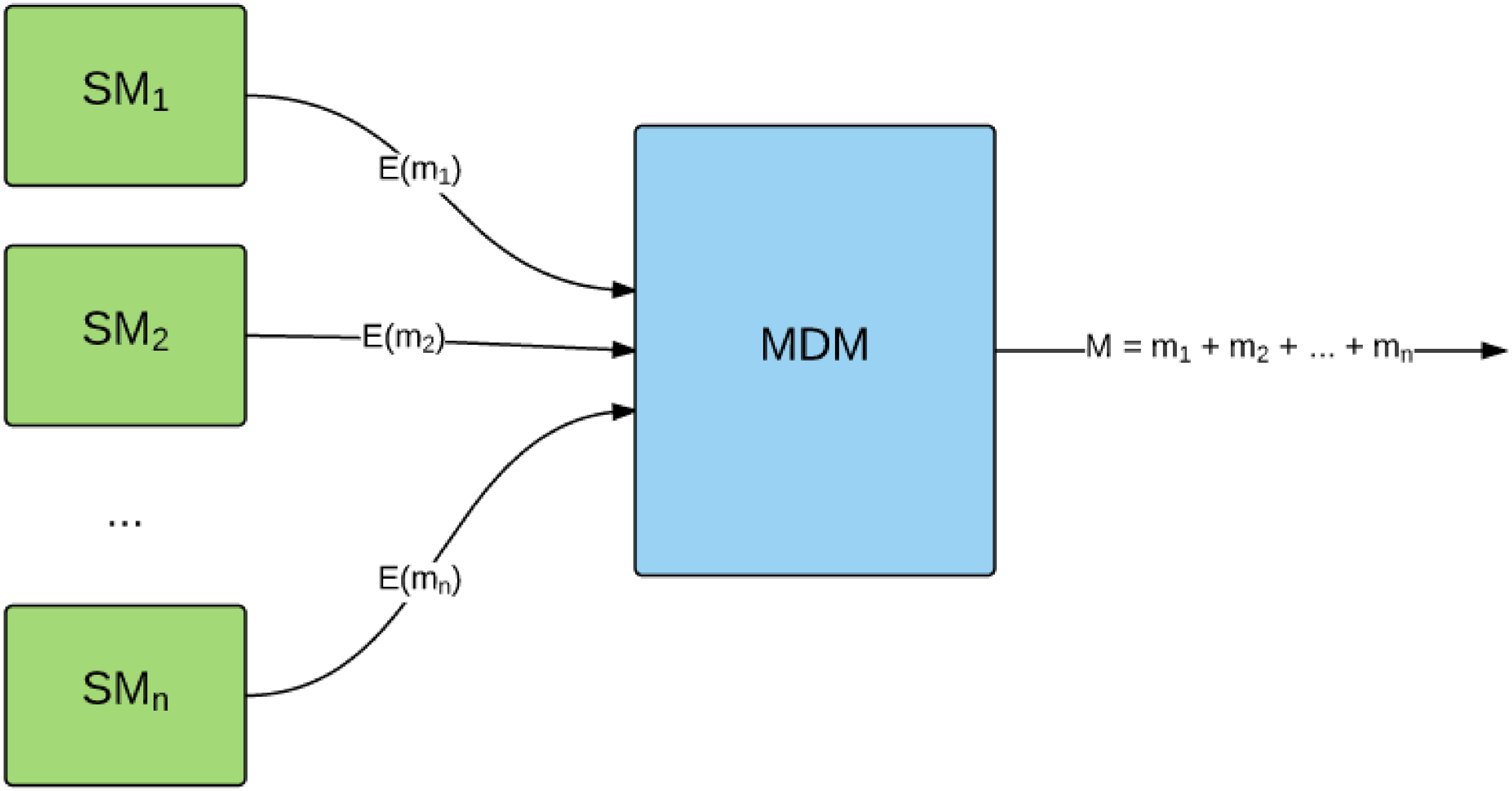
Criptografia Homomorfica em Smart Meters

Pedro Barbosa

2015

Problema



- Como calcular M?

Criptografia de Palier

- Seja $\boldsymbol{L(u) = (u - 1) / n}$
- Selecione $\boldsymbol{p}$ e $\boldsymbol{q}$ números primos grandes
- $\boldsymbol{n = p \cdot q}$
- $\boldsymbol{\lambda = mmc((p - 1) \cdot (q - 1))}$
- Selecione $\boldsymbol{g}$ um inteiro de $\boldsymbol{1}$ a $\boldsymbol{n^2}$ de forma que
- $\boldsymbol{b = L(g^{\lambda} (mod\ n^2))}$ seja coprimo a $\boldsymbol{n}$, ou seja, $\boldsymbol{mdc(b, n) = 1}$
- Por fim, $\boldsymbol{\mu}$ é o inverso multiplicativo de $\boldsymbol{b}$ módulo $\boldsymbol{n}$, ou seja, $\boldsymbol{\mu = b^{-1} (mod\ n)}$
- $\boldsymbol{P_k = (n, g)}$ e $\boldsymbol{S_k = (n, \lambda, \mu)}$

Criptografia de Palier

- Criptografia (de ***m***):
  - $r = rand[1, n-1]$
  - $c = g^m \cdot r^n \pmod{n^2}$
- Descriptografia (de ***c***):
  - $m = (L(c^\lambda \pmod{n^2}) \cdot \mu) \pmod{n}$
- Homomorfismo:
  - Considerando duas mensagens, temos $\mathbf{E(m_1 + m_2) = E(m_1) \cdot E(m_2)}$. Logo, o sistema de Paillier apresenta homomorfismo aditivo ao multiplicar blocos cifrados.

Criptografia de Palier

- Exemplo:
  - **p = 7, q=11**
  - $n = p \cdot q = 7 \cdot 11 \Rightarrow n = 77$
  - $\lambda = mmc\ ((p-1),(q-1)) = mmc\ (6, 10) \Rightarrow \lambda = 30$
  - $g = rand\ [1, n^2\ ]$, *tal que* , $mdc(b\ ,\ n) = 1$, *onde* $b = L(g^{\lambda}\ (mod\ n^2)) \Rightarrow g = 23$ *e* $b = 40$
  - $\mu = b^{-1}\ (mod\ n) \Rightarrow \mu \cdot 40\ (mod\ 77) = 1 \Rightarrow \mu = 52$
  - $P_k = (n\ ,\ g) \Rightarrow P_k = (77, 23)$
  - $S_k = (n\ ,\ \lambda\ ,\ \mu) \Rightarrow S_k = (77, 30, 52)$

Criptografia de Palier

- Criptografia:
  - **m=14**
  - ***r=rand [1, n−1] ⇒ r=69***
  - $c \equiv g^m \cdot r^n \pmod{n^2} \Rightarrow 2314 \cdot 6977 \pmod{772} \Rightarrow c = 3265$
- Descriptografia:
  - $c = 3265$
  - $m \equiv (L(c^\lambda \pmod{n^2}) \cdot \mu) \pmod{n} \Rightarrow m = (L(1618) \cdot 52) \pmod{77} \Rightarrow m=14$

Criptografia de Palier

- Homomorfismo:
  - Criptografia:
    - $\mathbf{m_1 = 14, m_2 = 3, m_3 = m_1 + m_2 = 17}$
    - $c_1 \equiv g^{m1} \cdot r^n \pmod{n^2} \Rightarrow c_1 \equiv 2314 \cdot 6977 \pmod{77^2} \Rightarrow c_1 = 3265$
    - $c_2 \equiv g^{m2} \cdot r^n \pmod{n^2} \Rightarrow c_2 \equiv 233 \cdot 26\ 77 (\bmod\ 77^2) \Rightarrow c_2 = 3503$
    - $c_3 = c_1 \cdot c_2 \Rightarrow c_3 = 11437295$
  - Descriptografia:
    - $m_3 \equiv (L(c_3{}^\lambda \pmod{n^2}) \cdot \mu) \pmod{n} \Rightarrow m_3 = (L(4929) \cdot 52) \pmod{77} \Rightarrow m_3 = 17$

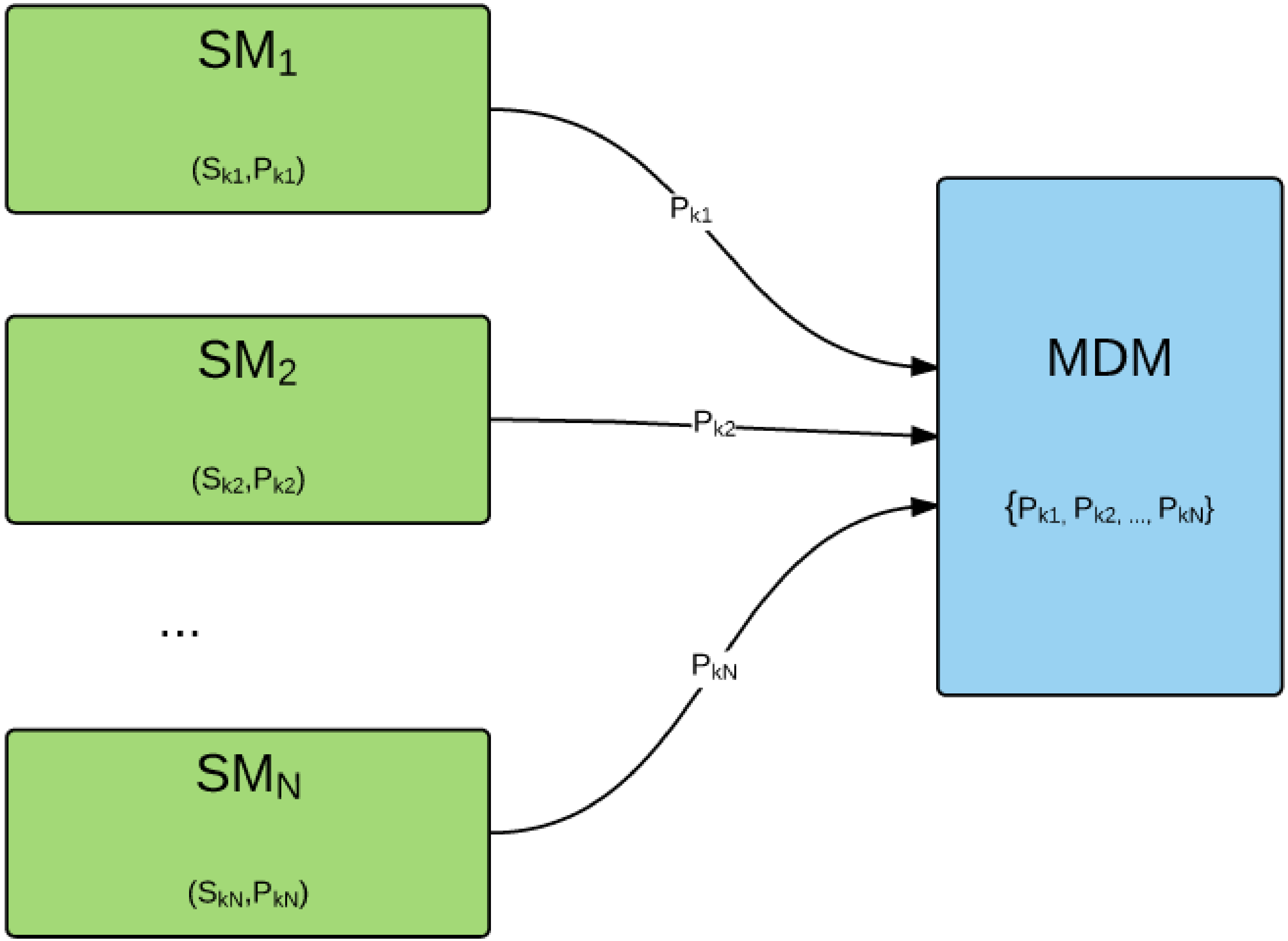
Privacidade em Smart Metering por Garcia et al.

1- Cada medidor possui uma chave pública $\boldsymbol{P_{ki}}$ e uma privada $\boldsymbol{S_{ki}}$ de Pailier

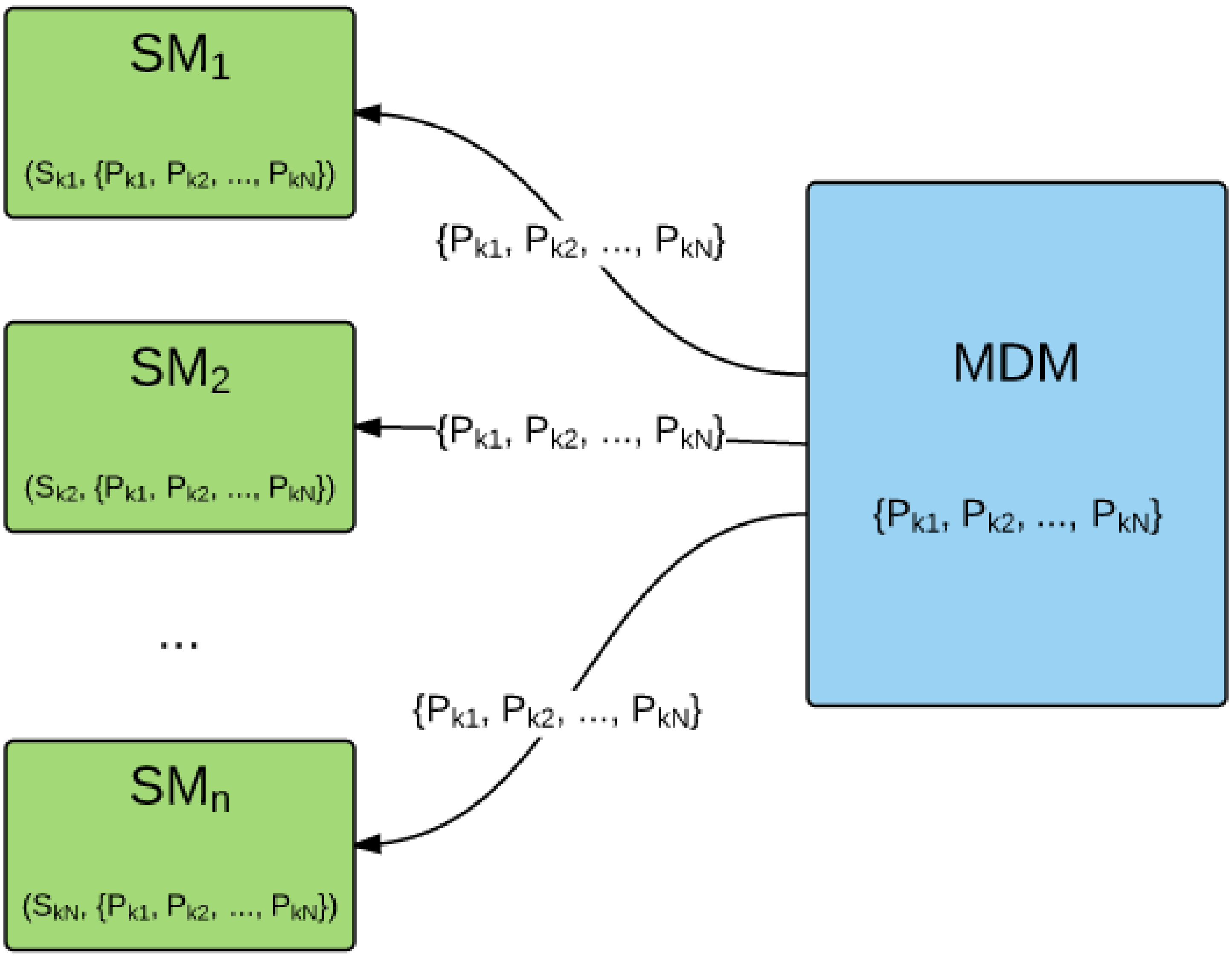
2- A concessionária obtém as chaves públicas de todos os medidores e compartilha este grupo de chaves públicas com todos os medidores.

- Cada medidor fica com a sua chave privada $\boldsymbol{S_{ki}}$, e todas as chaves públicas $\boldsymbol{\{P_{k1}, \ldots, P_{kN}\}}$.

Privacidade em Smart Metering por Garcia et al.



Privacidade em Smart Metering por Garcia et al.



Privacidade em Smart Metering por Garcia et al.

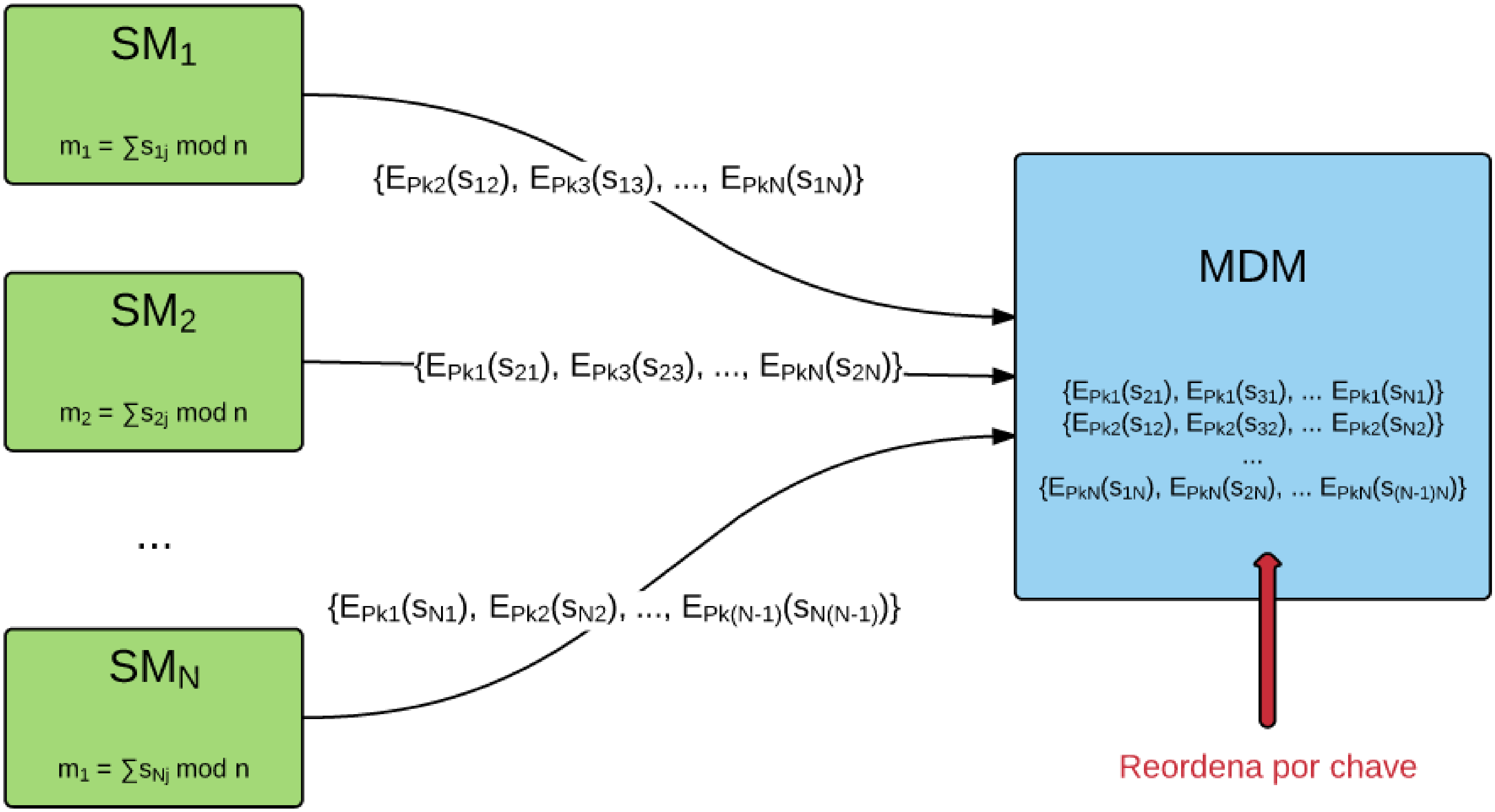
3- Cada medidor $\boldsymbol{SM_i}$ calcula para a sua medição $\boldsymbol{m_i}$, $\boldsymbol{N}$ segredos compartilhados, de forma que

$$m_i = \sum_j s_{ij}$$ para um ***n*** grande.

4- $\boldsymbol{SM_i}$ armazena $\boldsymbol{s_{ii}}$ para si mesmo e envia para a concessionária os outros segredos compartilhados criptografados com as chaves públicas dos outros ***N-1*** medidores

– Ou seja, envia $\boldsymbol{E_{Pkj}(s_{ij})}$ para $\boldsymbol{j = 1, \ldots, i-1, i+1, \ldots, N}$.

Privacidade em Smart Metering por Garcia et al.



Privacidade em Smart Metering por Garcia et al.

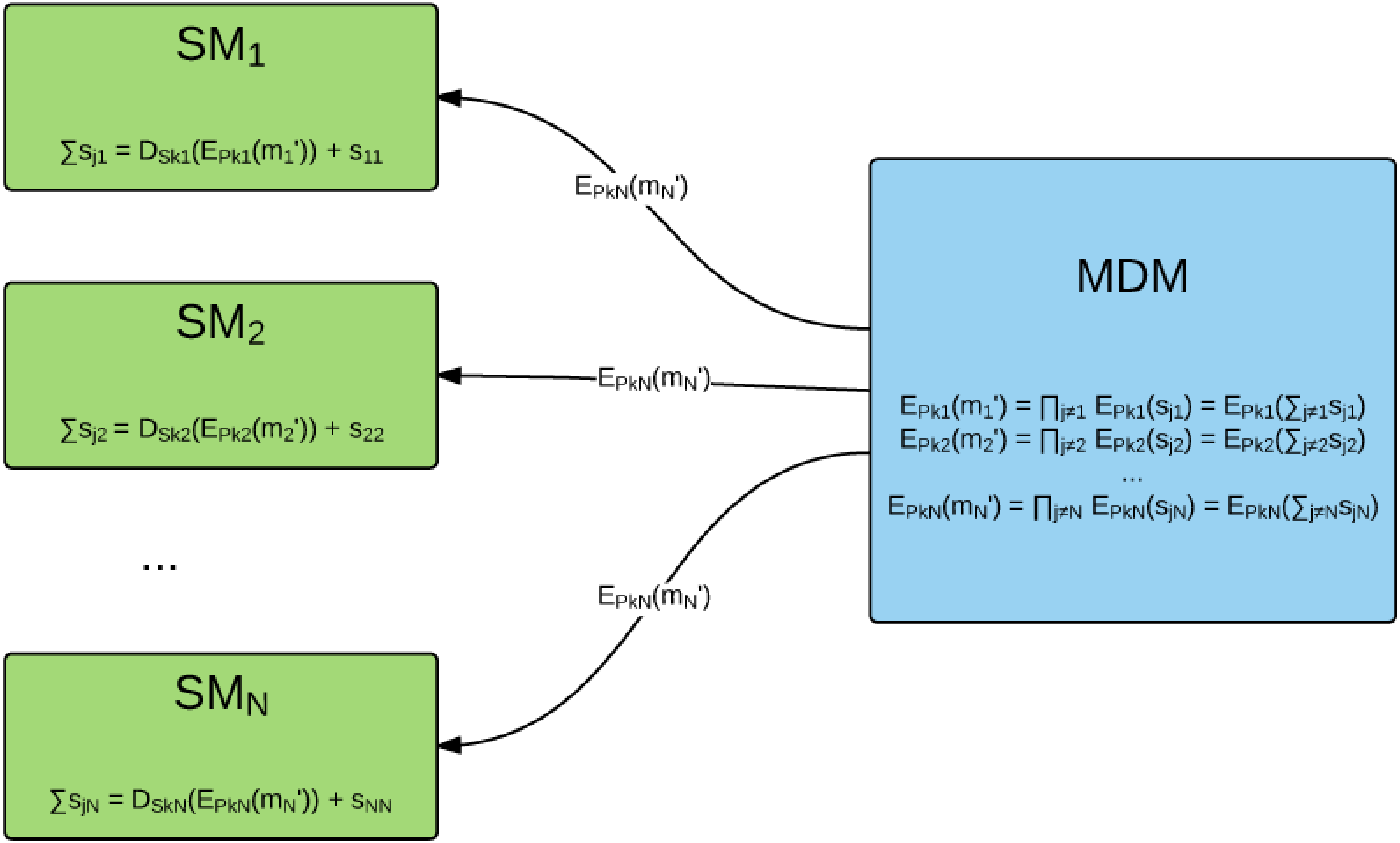
5- Ao receber todos os segredos compartilhados criptografados, a concessionária multiplica os que foram criptografados com a mesma chave pública. Devido a propriedade homomórfica, tem-se para cada *i*:

$$E_{P_{ki}}(m_i{}') = \prod_{j \neq i} E_{P_{ki}}(s_{ji}) = E_{P_{ki}}\left(\sum_{j \neq i} s_{ji}\right)$$

6- A concessionária envia $\boldsymbol{E_{Pki}(m_i')}$ para o medidor $\boldsymbol{SM_i}$, que pode descriptografar com a sua chave privada $\boldsymbol{S_{ki}}$ e adicionar o segredo $\boldsymbol{s_{ii}}$. Assim, o medidor obtém:

$$\sum_j s_{ji}$$

Privacidade em Smart Metering por Garcia et al.

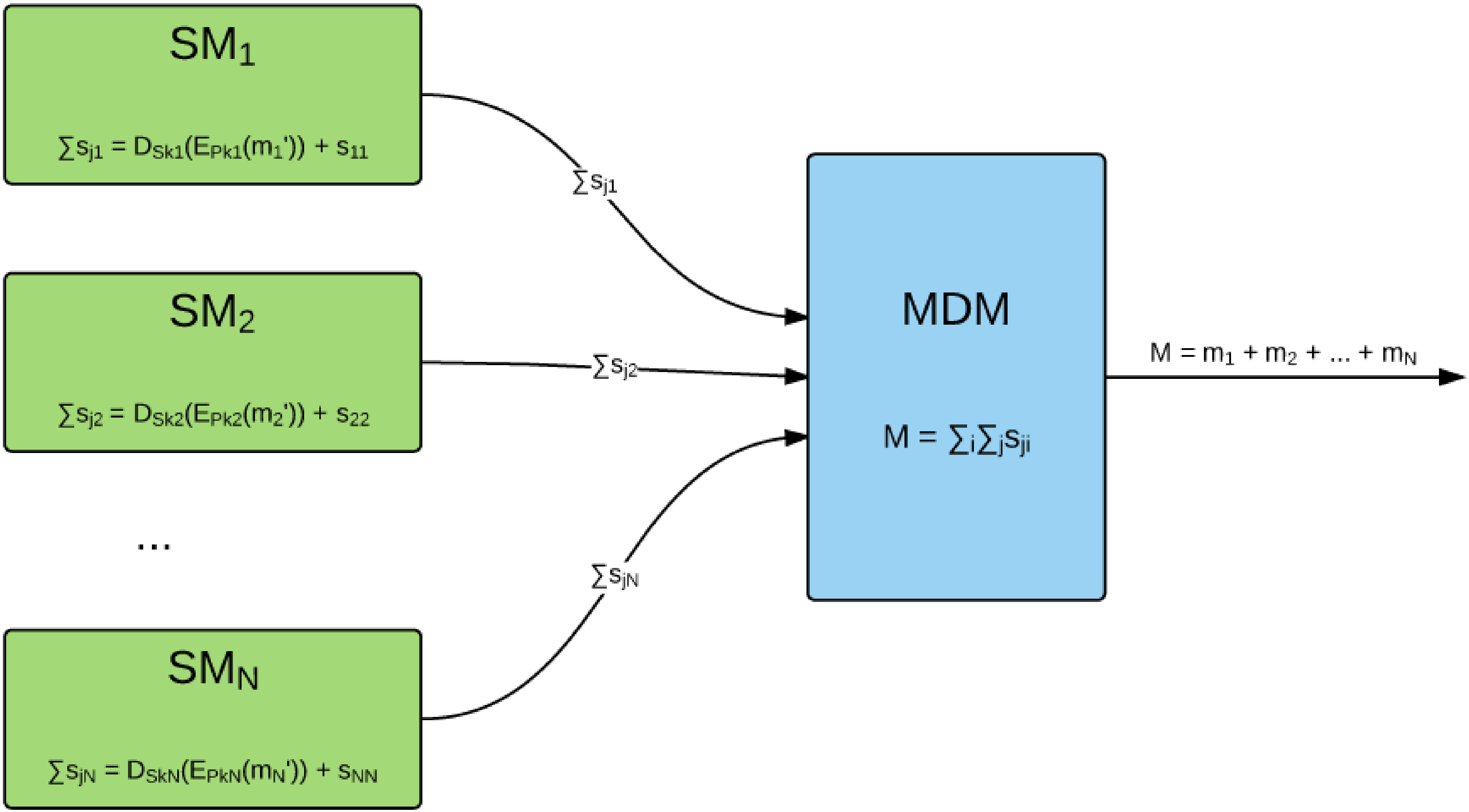


Privacidade em Smart Metering por Garcia et al.

7- O medidor ***SMᵢ*** então envia $\sum_j s_{ji}$ para a concessionária, que ao somar os resultados recebidos de todos os medidores obterá o consumo total ***M*** da região

$$M = \sum_i \sum_j s_{ji} \mod n$$

Privacidade em Smart Metering por Garcia et al.



Privacidade em Smart Metering por Garcia et al.

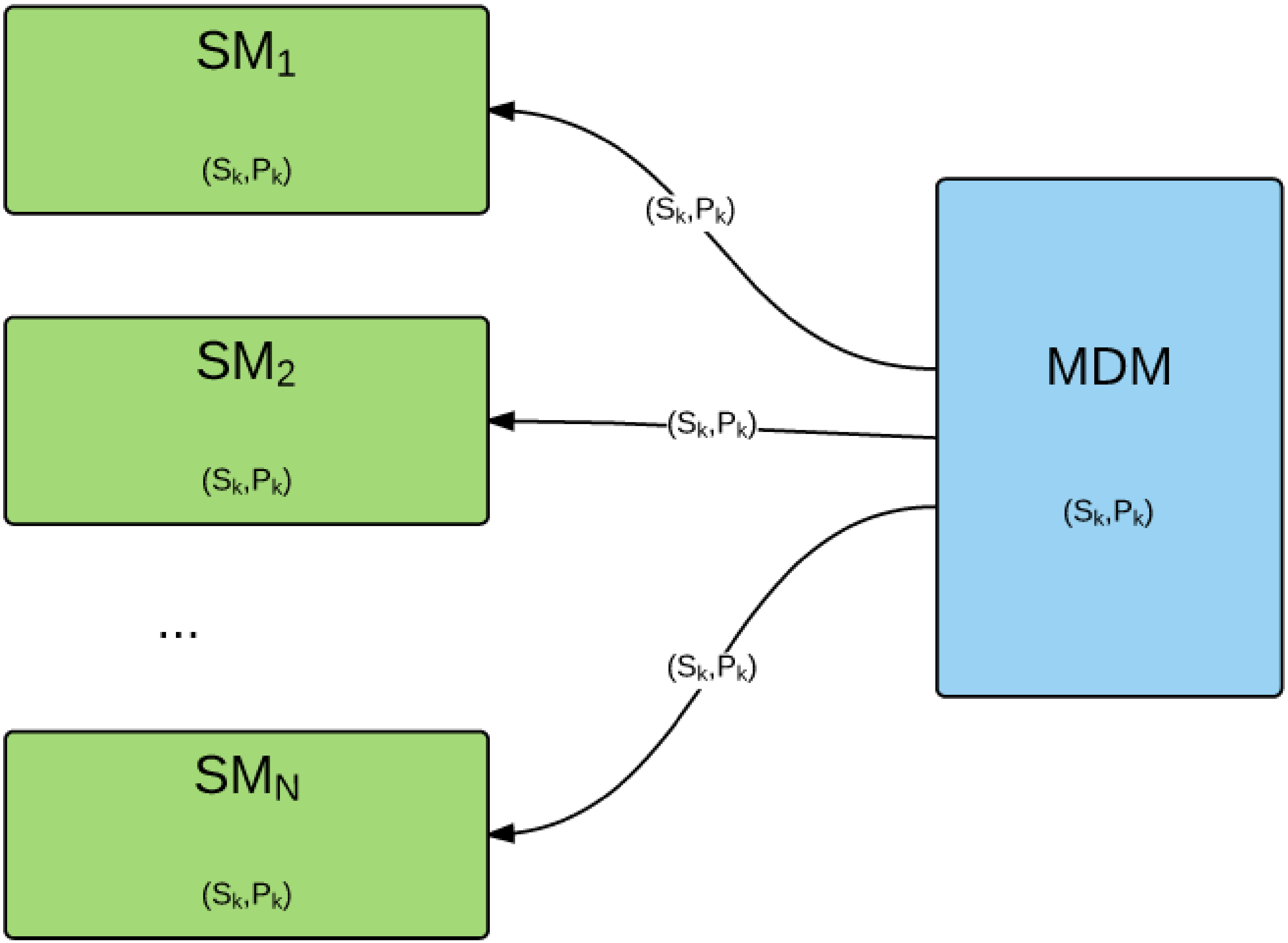
- Problemas:
  - Muita troca de mensagens entre um medidor e a concessionária (5 mensagens)
  - Não é escalável:
    - Se um único medidor falhar durante dos passos, não se obtém nem mesmo uma aproximação
  - Considerando geração de chaves, criptografia, descriptografia e geração de segredos como O(1), temos:
    - ***O(N)*** para cada medidor (passos 3 e 4)
    - ***O(N²)*** para a concessionária (passo 5)

Privacidade em Smart Metering por Erkin et al.

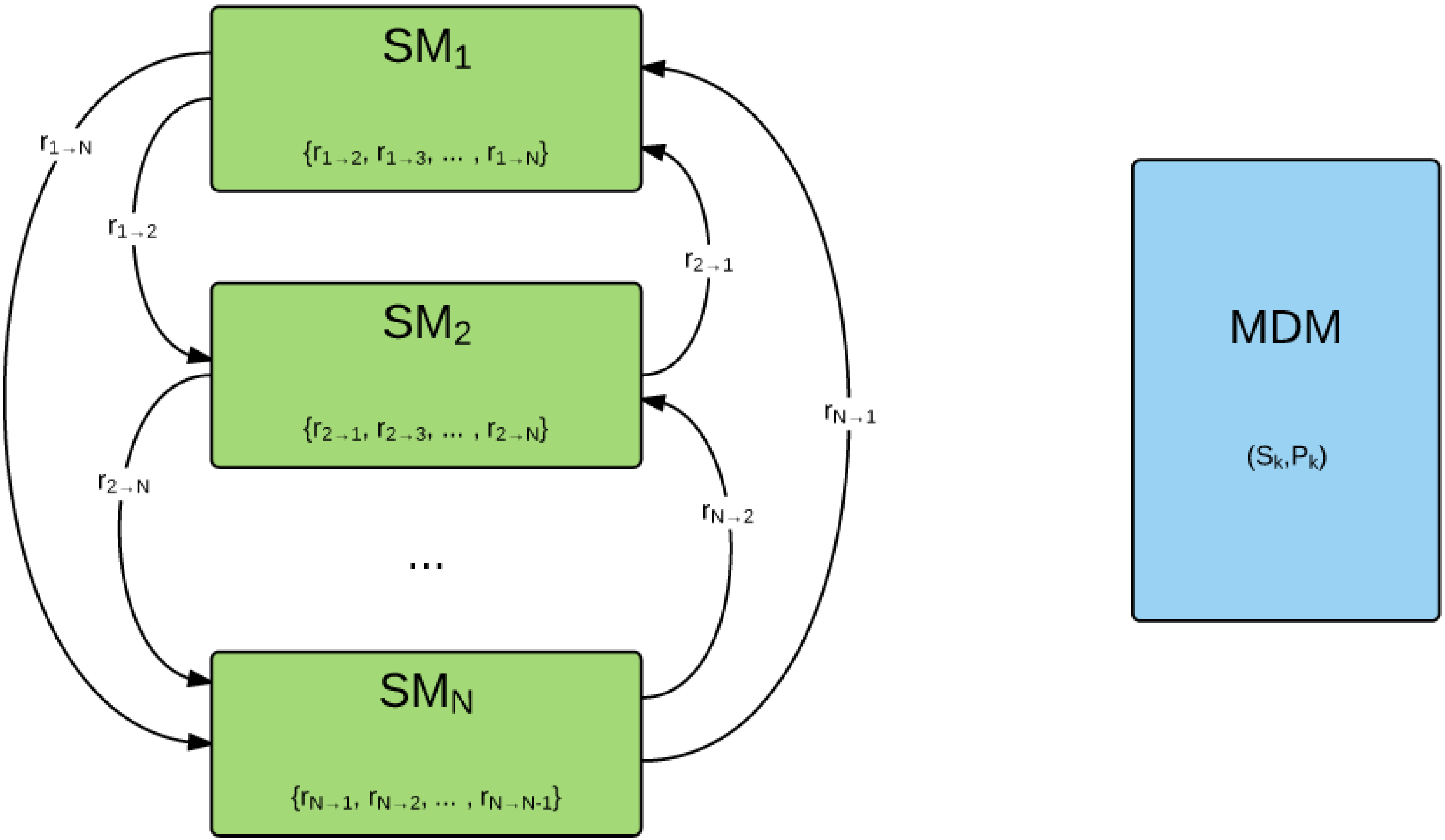
1- Um único par de chaves do esquema de Paillier é compartilhado entre todos os ***N*** medidores (i.e, todos os medidires possuem $\boldsymbol{P_k}$ e $\boldsymbol{S_k}$)

2- Para uma medição $\boldsymbol{m_i}$, o medidor $\boldsymbol{SM_i}$ gera ***N - 1*** números aleatórios, um para cada outro medidor, e os distribui utilizando canais seguros (ex, criptografia assimétrica RSA na comunicação entre medidores).

Privacidade em Smart Metering por Erkin et al.



Privacidade em Smart Metering por Erkin et al.



Privacidade em Smart Metering por Erkin et al.

3- Após receber todos os números aleatórios gerados pelos outros medidores, $\boldsymbol{SM_i}$ computa:

$$R_i = n + \sum_{j=1, i \neq j}^{N} r_{(i \to j)} - \sum_{j=1, i \neq j}^{N} r_{(j \to i)}$$

- Onde $\boldsymbol{n}$ é o módulo usado em Paillier e $\boldsymbol{r_{i \to j}}$ é o número aleatório gerado de $\boldsymbol{SM_i}$ para $\boldsymbol{SM_j}$

4- Em seguida computa-se um hash $\boldsymbol{h_t}$ utilizando o timestamp da medição atual ($\boldsymbol{m_i}$). Este hash precisa ser coprimo a $\boldsymbol{n}$, ou seja, $\boldsymbol{mdc(h_t, n)=1}$.

- Como o timestamp é sincronizado para todos os medidores, espera-se que o hash obtido seja o mesmo para todos.

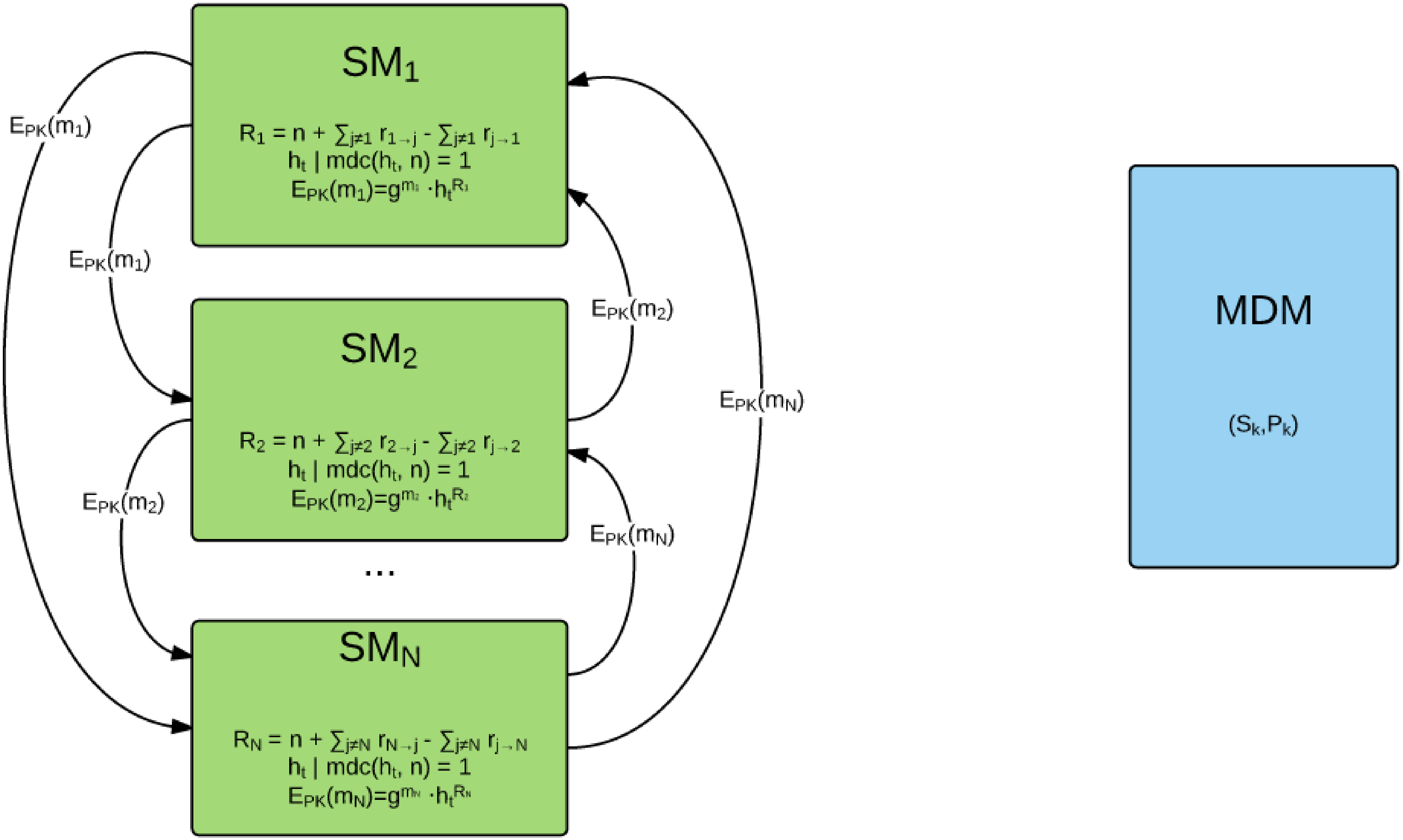
Privacidade em Smart Metering por Erkin et al.

5- Após o medidor computar $\boldsymbol{R_i}$ e $\boldsymbol{h_t}$, criptografa-se a medição $\boldsymbol{m_i}$ utilizando o seguinte esquema modificado de Paillier:

$$E_{P_k}(m_i) = g^{m_i} \cdot h_t^{R_i}$$

- Em seguida esta mensagem criptografada é disseminada para todos os outros ***N-1*** medidores.

Privacidade em Smart Metering por Erkin et al.



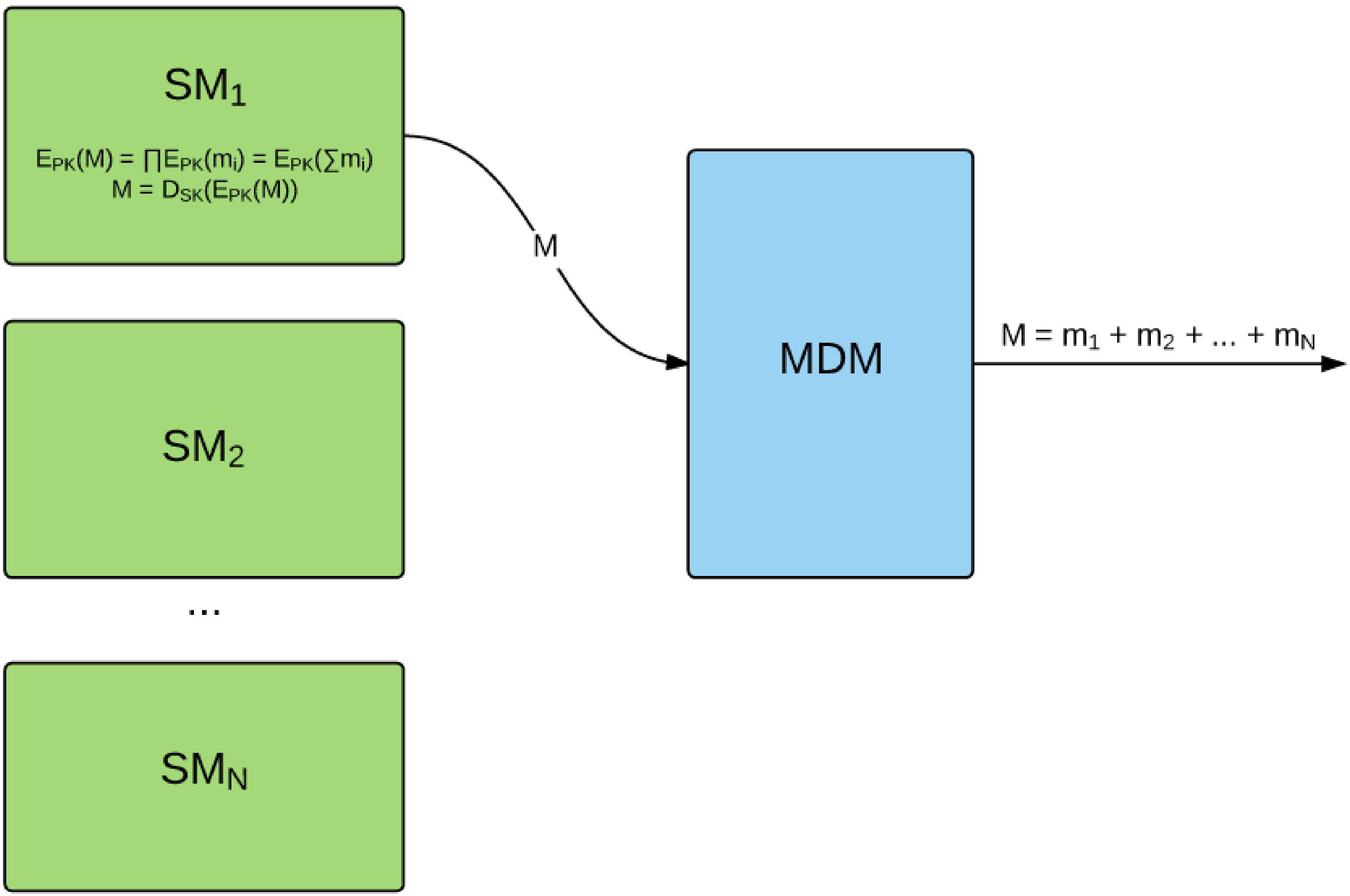
Privacidade em Smart Metering por Erkin et al.

6- Quando um medidor receber todas as medições criptogradas dos outros medidores, ele poderá calcular o consumo total na região devido a propriedade homomórfica:

$$E_{P_k}(M) = \prod_{i=1}^{N} E_{P_k}(m_i) = E_{P_k}\left(\sum_{i=1}^{N} m_i\right)$$

– Ao descriptografar $\boldsymbol{E_{Pk}(M)}$, o medidor poderá enviar o valor $\boldsymbol{M}$ para a concessionária.

Privacidade em Smart Metering por Erkin et al.



Privacidade em Smart Metering por Erkin et al.

- Por que funciona?
  - Um medidor não consegue descriptografar medições individuais dos outros
    - Ele só possui os números aleatórios gerados por ele e os gerados para ele

$$E_{P_k}(m_i) = g^{m_i} \cdot h_t^{R_i} \qquad R_i = n + \sum_{j=1, i \neq j}^{N} r_{(i \to j)} - \sum_{j=1, i \neq j}^{N} r_{(j \to i)}$$

  - A descriptografia do agregado funciona, pois:

$$E_{P_k}(M) = g^{m_1 + m_2 + \ldots + m_N} \cdot h_t^{\sum_{i=1}^{N} n + \sum_{i=1}^{N} \sum_{j=1, i \neq j}^{N} r_{(i \to j)} - \sum_{i=1}^{N} \sum_{j=1, i \neq j}^{N} r_{(j \to i)}}$$

Privacidade em Smart Metering por Erkin et al.

$$E_{P_k}(M) = g^M \cdot h_t^{N \cdot n}$$

- Ora, sendo $\boldsymbol{r = h_t^N}$ como um número aleatório, temos a configuração de Paillier original

Privacidade em Smart Metering por Erkin et al.

- Problemas:
  - Muita troca de mensagens entre medidores (2N - 2 mensagens) e duas com a concessionária
  - Não é escalável:
    - Se um único medidor falhar durante dos passos, não se obtém nem mesmo uma aproximação
  - Considerando geração de chaves, criptografia, descriptografia e geração de segredos como O(1), temos:
    - ***O(N)*** para cada medidor (passos 2, 3 e 6)
    - ***O(N)*** para a concessionária (passo 1)
      - Mas poderia ser O(1) (cada medidor salvaria o par de chaves)

Criptografia de ElGamal

- Problema do logaritmo discreto:
  - Seja $\boldsymbol{G}$ um grupo multiplicativo de ordem $\boldsymbol{p}$ e seja $\boldsymbol{g}$ um gerador de $\boldsymbol{G}$
  - Dado $\boldsymbol{g}$ e $\boldsymbol{y}$, como encontrar o inteiro $\boldsymbol{x}$ tal que $\boldsymbol{g^x = y}$?
  - Tal inteiro $\boldsymbol{x}$ é o logaritmo discreto de $\boldsymbol{y}$ na base $\boldsymbol{g}$ ($\boldsymbol{\log_g y = x}$)
- Problema computacional de Diffie-Hellman:
  - Seja $\boldsymbol{G}$ um grupo multiplicativo.
  - Dado $\boldsymbol{g^a}$ e $\boldsymbol{g^b}$ com $\boldsymbol{a}$ e $\boldsymbol{b}$ desconhecidos, como computar $\boldsymbol{g^{ab}}$?

Criptografia de ElGamal

- Seja q um número primo grande
- Seja g um gerador do grupo multiplicativo G de ordem q (i.e, $\mathbb{Z}^*_q$)
- Obter $x = rand(G)$ e $y = g^x$
- $S_k = x$ e $P_k = (G, g, y)$
- Para criptografar uma mensagem $m \in G$, obtém-se $r = rand(G)$ e computa-se $c = g^r$ e $d = m.y^r$. Assim, $E(m) = (c,d)$
- Para descriptografar $E(m)$ computa-se $m = d.c^{-x}$

Criptografia de ElGamal

- Propriedade homomórfica:
  - Seja $\boldsymbol{E(m_1) = (c_1, d_1) = (g^{r1}, m_1.y^{r1})}$ e $\boldsymbol{E(m_2) = (c_2, d_2) = (g^{r2}, m_2.\ y^{r2})}$
  - Assim, $\boldsymbol{E(m_1)\ .\ E(m_2) = (c_1.c_2, d_1.d_2) = (g^{r1 + r2}, m_1.\ m_2.y^{r1 + r2}) = E(m_1\ .\ m_2)}$
- Ou seja, ElGamal é um sistema homomórfico multiplicativo

Criptografia de ElGamal

- Dado $E(g^{m1})$ e $E(g^{m2})$, então $E(g^{m1}) . E(g^{m2}) = E(g^{m1} . g^{m2}) = E(g^{m1 + m2})$
- Assim, também pode-se obter a propriedade homomórfica aditiva se conseguir computar ***m*** em $m' = g^m$.
  - Por exemplo, na espanha o consumo de um consumidor durante 30 min fica em torno de 0 – 7500 Wh. Para 128 medidores é necessário números de 20-bits. Em um Intel Core 2.5GHz e 4GB RAM, levou-se em média 0.046s.
  - Assim, sabendo-se o range, o cálculo do logaritmo discreto não fica tão custoso.

Privacidade em Smart Metering por Busom et al.

1- Cada medidor possui:

- O número primo grande $\boldsymbol{q}$ e o gerador $\boldsymbol{g}$ (já vem em hardware e de fábrica)
- Uma chave privada $\boldsymbol{x_i}$
- Uma chave pública $\boldsymbol{y_i = g^{x_i}}$ e um certificado $\boldsymbol{Cert_i}$
- A chave pública da autoridade certificadora que verifica os certificados dos outros medidores.

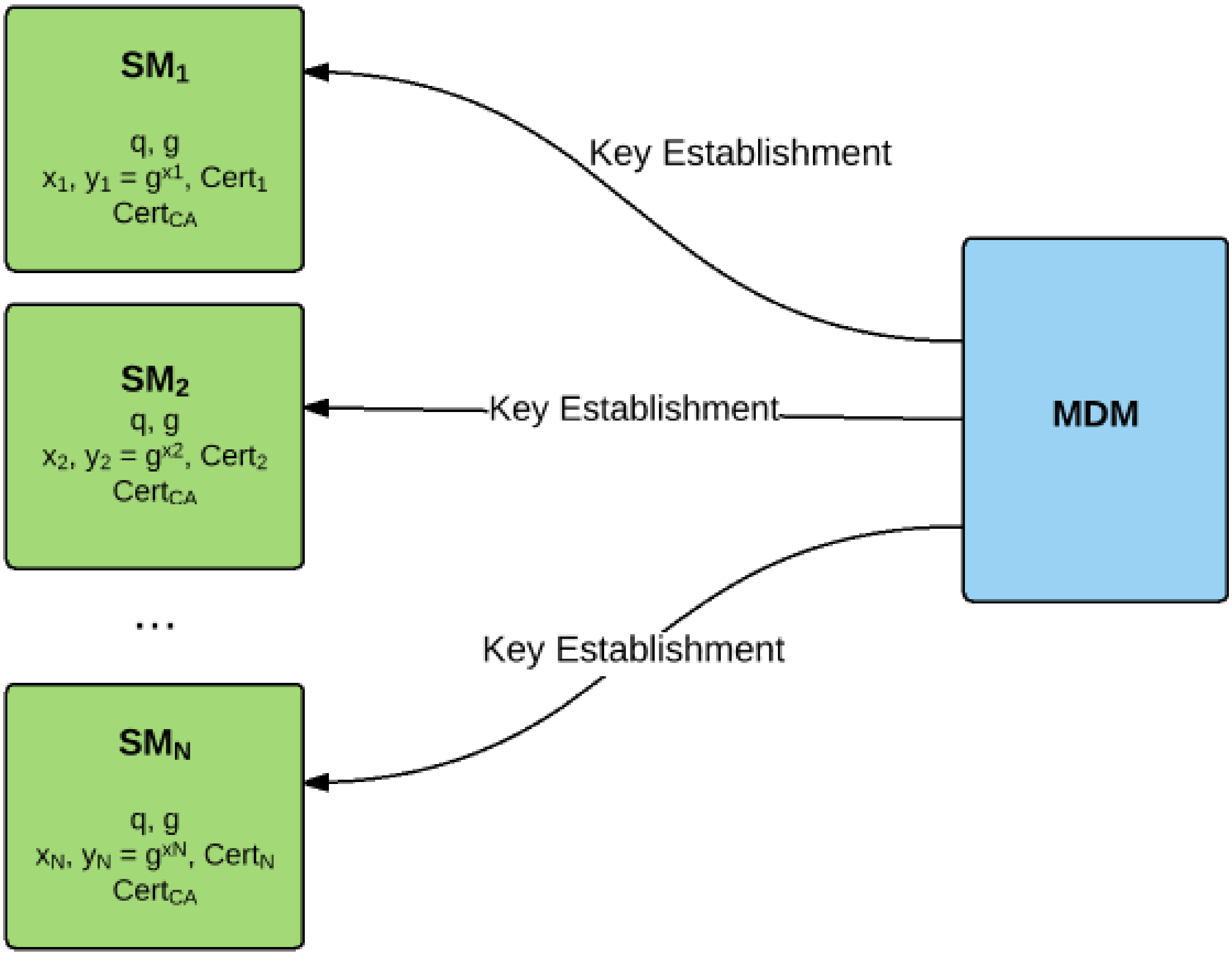
Privacidade em Smart Metering por Busom et al.

2- Quando se tem uma nova configuração (ex, novo medidor na região), a concessionária inicia um procedimento de estabelecimento de chaves:

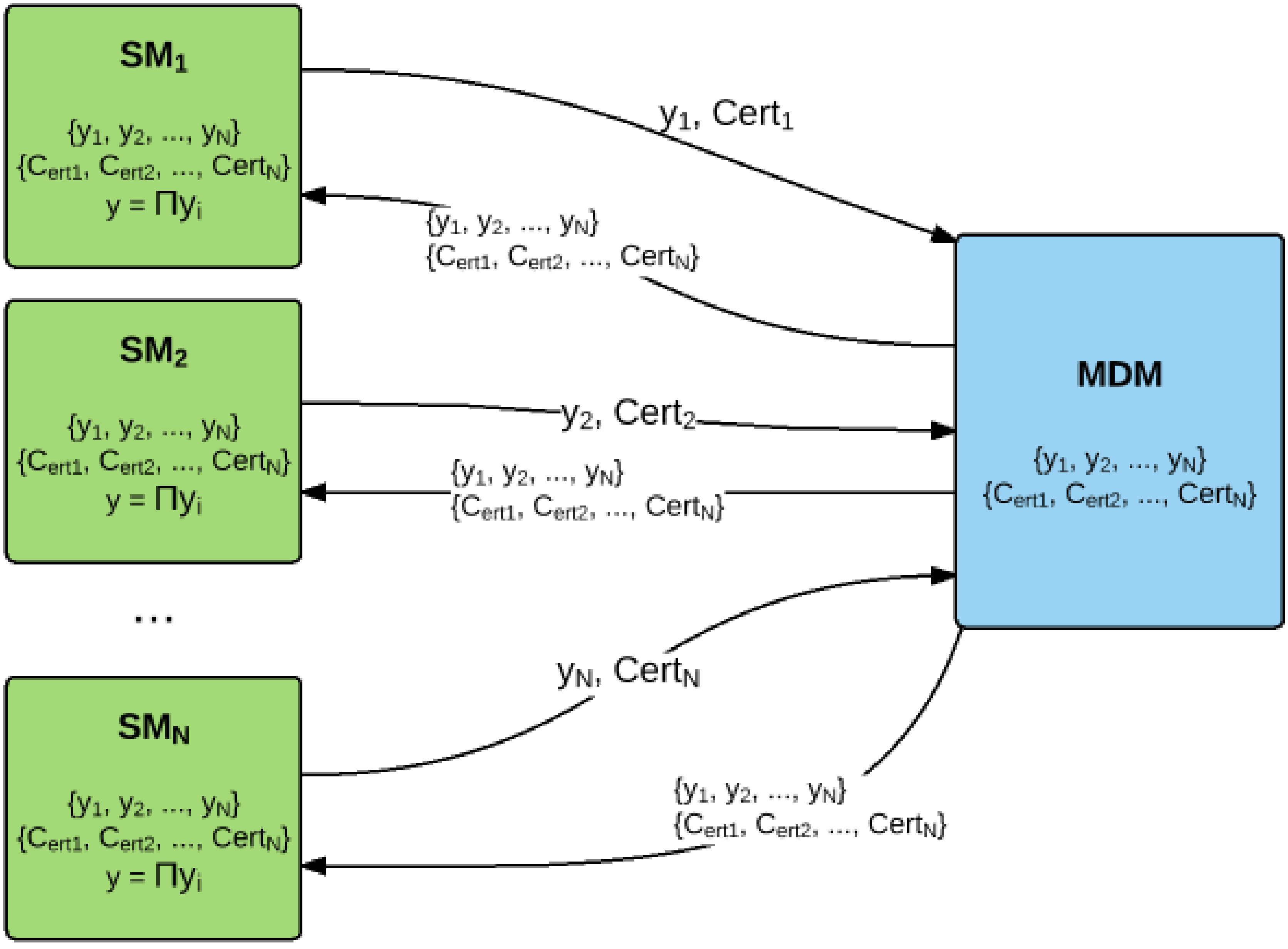
- A concessionária envia uma mensagem de key establishment para cada um dos medidores
- Cada medidor envia $\boldsymbol{y_i}$ e $\boldsymbol{Cert_i}$ para a concessionária
- A concessionária verifica a validade de cada $\boldsymbol{Cert_i}$ e envia $\boldsymbol{\{y_1, \ldots, y_n\}}$ e $\boldsymbol{\{Cert_1, \ldots, Cert_n\}}$ para cada medidor
- Finalmente, cada um dos medidores verifica a validade de cada $\boldsymbol{Cert_i}$ e computa uma chave pública global:

$$y = \prod_{i=1}^{N} y_i$$

Privacidade em Smart Metering por Busom et al.



Privacidade em Smart Metering por Busom et al.



Privacidade em Smart Metering por Busom et al.

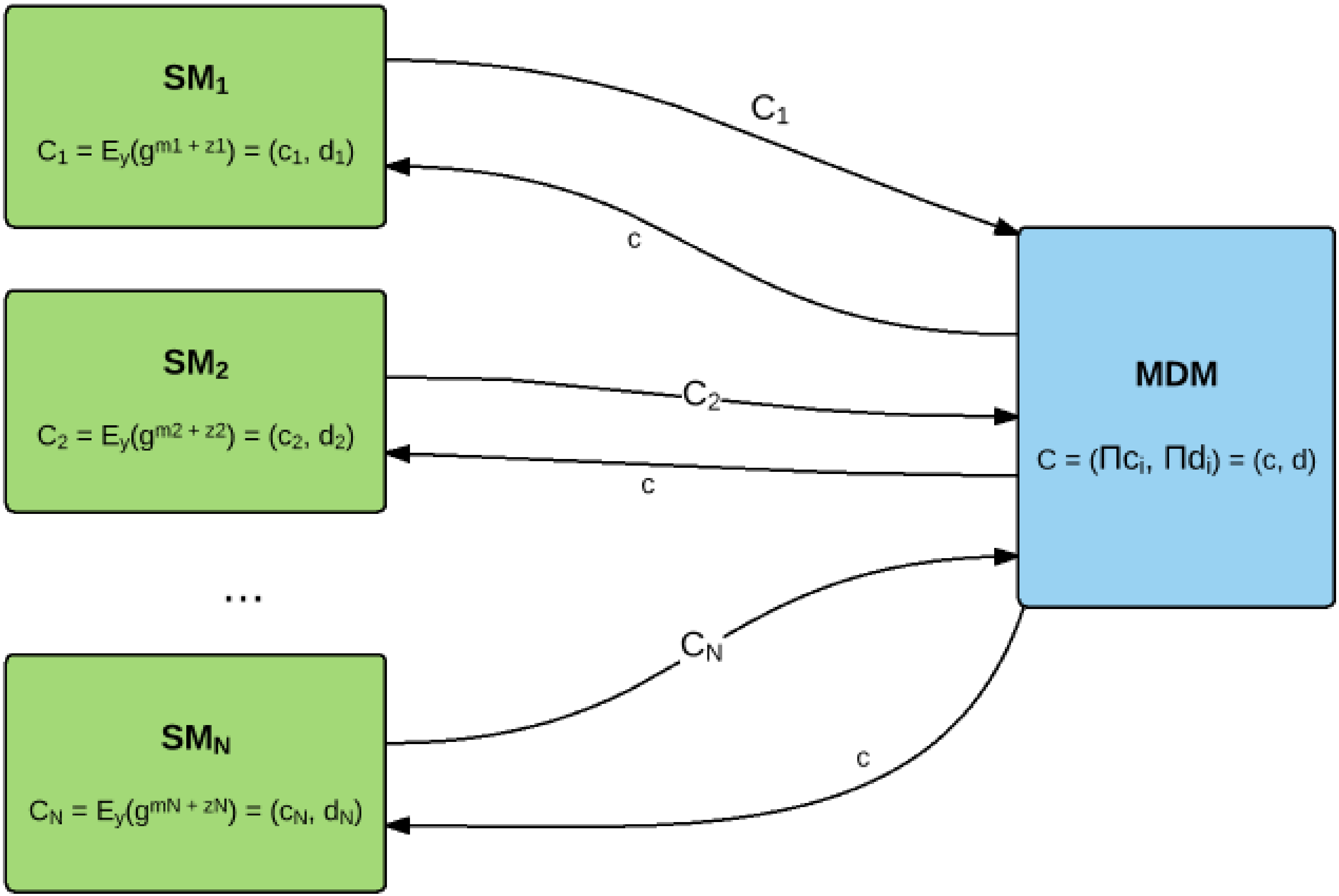
3- A cada instante, a concessionária envia para os medidores requisições de medição e cada medidor gera um número aleatório $z_i \in \mathbb{Z}^*_q$, computa $C_i = E_y(g^{m_i + z_i}) = (c_i, d_i)$ e envia C_i para a concessionária

4- A concessionária agrega todos os C_i recebidos:

$$C = \left(\prod_{i=1}^{N} c_i, \prod_{i=1}^{N} d_i\right) = (c, d)$$

e envia ***c*** para cada medidor.

Privacidade em Smart Metering por Busom et al.



Privacidade em Smart Metering por Busom et al.

5- Cada medidor computa $\boldsymbol{T_i = c^{x_i} . g^{z_i}}$ e envia o resultado para a concessionária

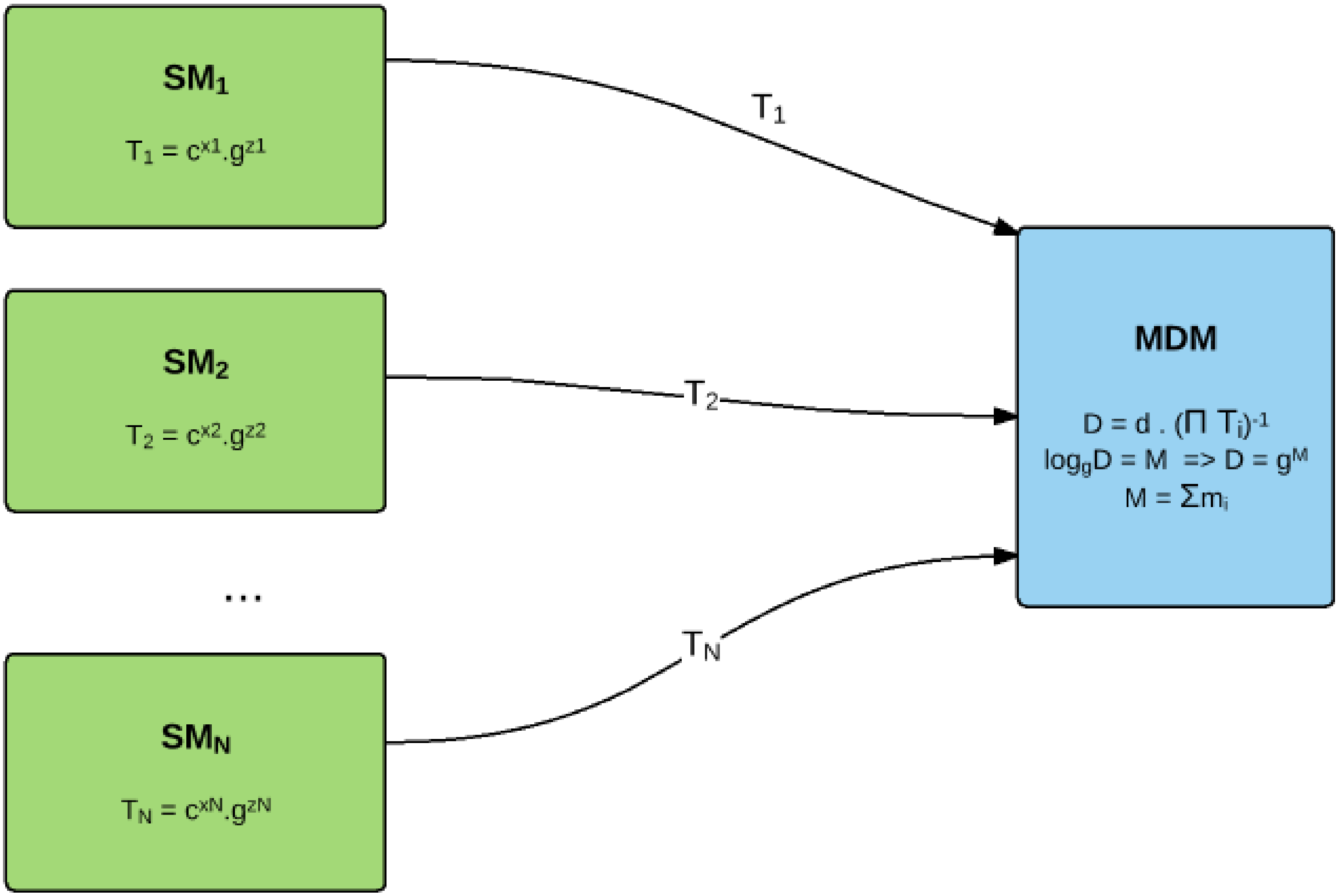
6- A concessionária então computa

$$D = d \cdot \left(\prod_{i=1}^{N} T_i \right)^{-1}$$

e finalmente computa $\boldsymbol{\log_g D}$, obtendo

$$D = g^M \qquad M = \sum_{i=1}^{N} m_i$$

Privacidade em Smart Metering por Busom et al.



Privacidade em Smart Metering por Busom et al.

- Por que funciona?
  - Primeiro cada medidor calcula
    $C_i = E_y(g^{mi+zi}) = (g^{ri}, g^{mi+zi} \, . \, y^{ri})$
  - Em seguida a concessionária calcula

$$C = \left(\prod_{i=1}^{N} g^{ri}, \prod_{i=1}^{N} g^{mi+zi} \cdot y^{ri} \right) = \left(g^{r}, g^{m+z} \cdot y^{r} \right) = (c, d)$$

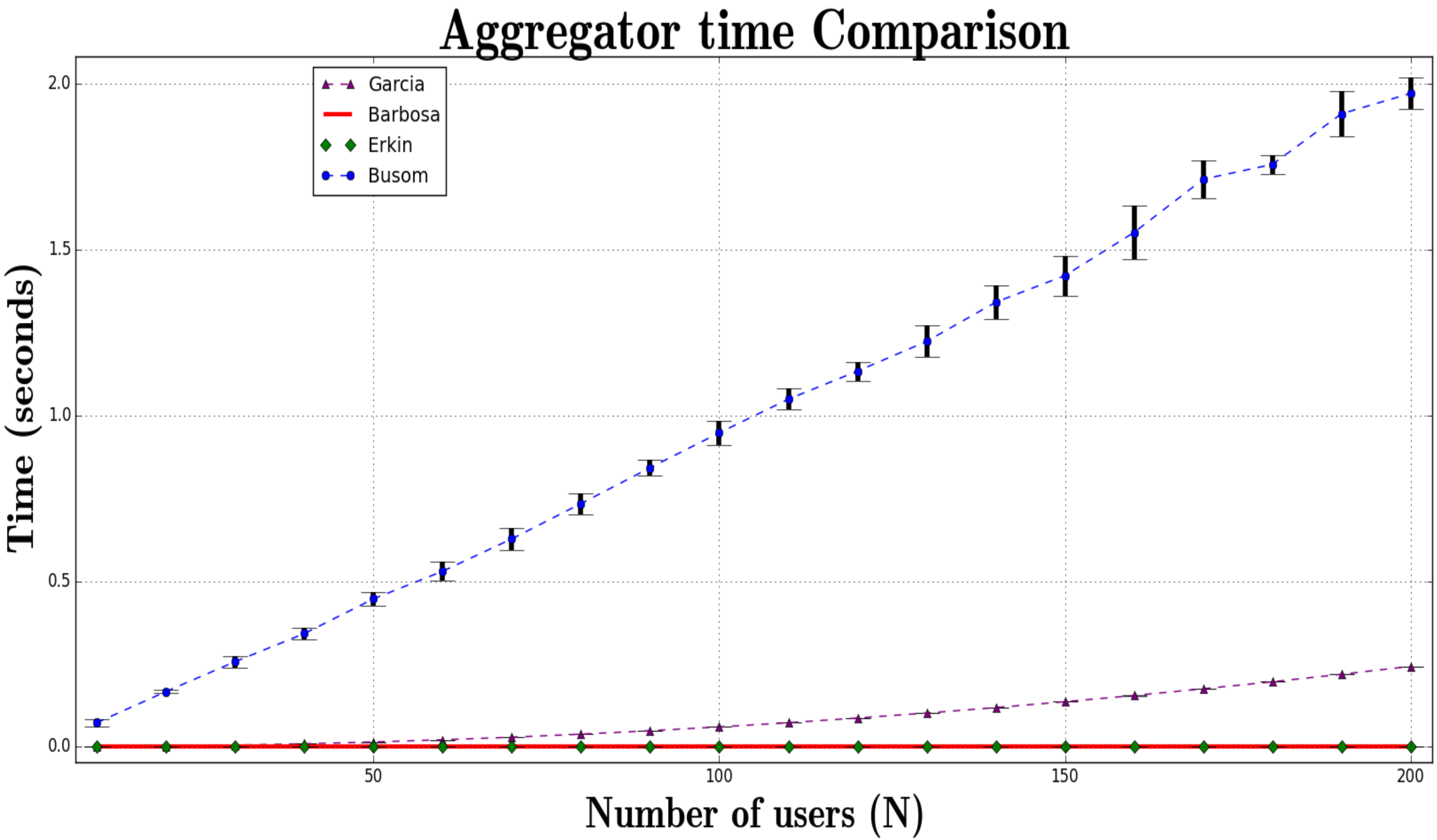
  - Depois cada medidor calcula
    $T_i = c^{xi} \, . \, g^{zi} = g^{r \, . \, xi} \, . \, g^{zi} = g^{xi \, . \, r} \, . \, g^{zi} = y_i^r \, . \, g^{zi}$

$$D = d \cdot \left(\prod_{i=1}^{n} T_i \right)^{-1} = \frac{g^{m+z} \cdot y^r}{\prod_{i=1}^{n} (y_i^r \cdot g^{z_i})} = \frac{g^{m+z} \cdot y^r}{(\prod_{i=1}^{n} y_i^r) \cdot g^z} = \frac{g^{m+z} \cdot y^r}{g^z \cdot y^r} = g^m$$

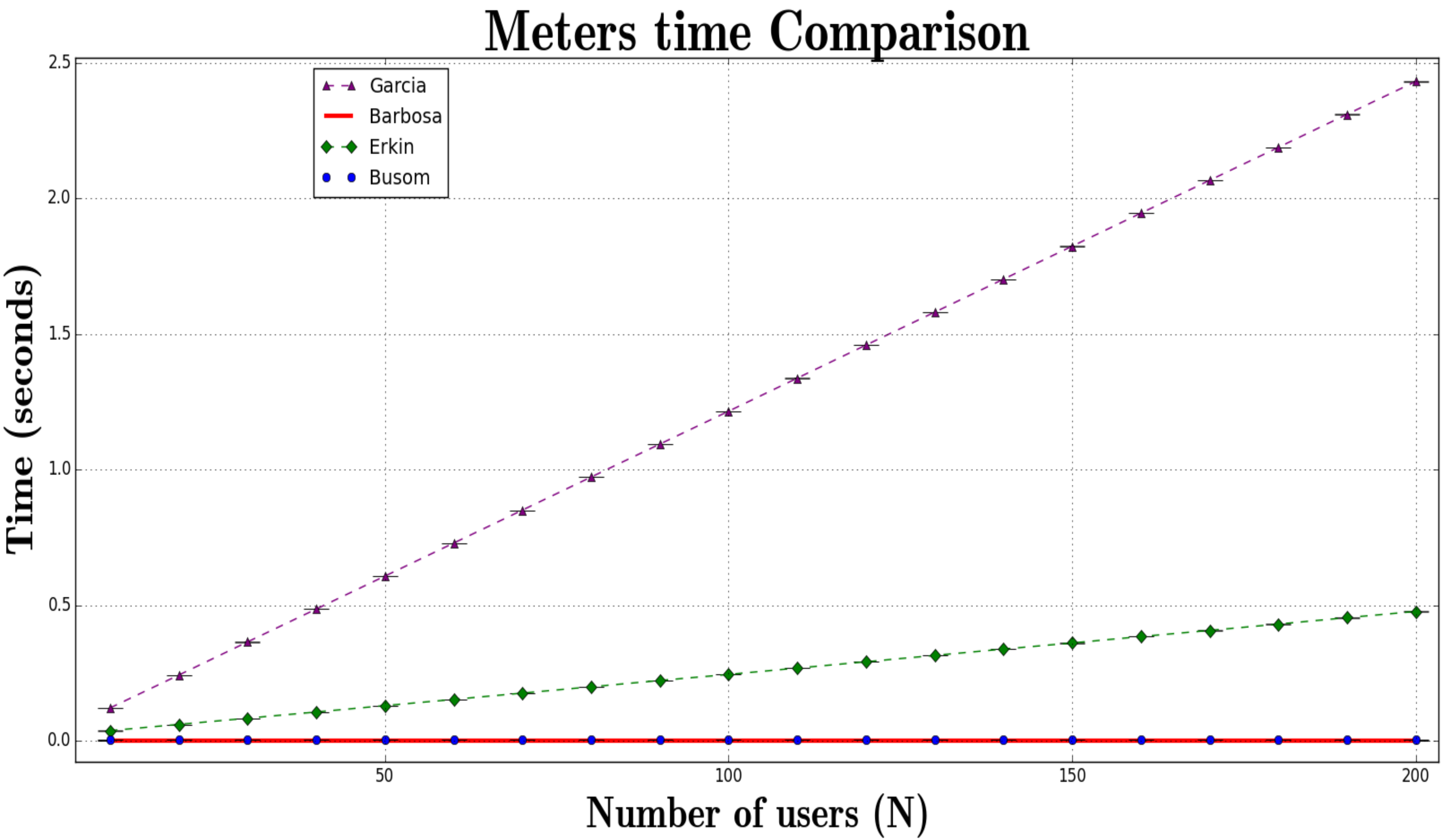
Privacidade em Smart Metering por Busom et al.

- Problemas:
  - Muita troca de mensagens entre um medidor e a concessionária (3 mensagens)
  - Não é escalável:
    - Se um único medidor falhar durante dos passos, não se obtém nem mesmo uma aproximação
  - Considerando geração de chaves, criptografia, descriptografia e geração de segredos como O(1), temos:
    - ***O(1)*** para cada medidor (mas no key establishment é ***O(N)***)
    - ***O(N)*** para a concessionária (passos 4 e 6)

Privacidade em Smart Metering



Privacidade em Smart Metering



Criptografia de Curva Elíptica

- Criptografia assimétrica
- Mais rápida e usa chaves mais curtas do que os métodos antigos como RSA, proporcionando ao mesmo tempo um nível de segurança equivalente
- Baseada na suposição de que é difícil encontrar um inteiro ***k***, tal que ***Q = k . P***, onde ***P*** e ***Q*** são dois pontos em uma curva elíptica
- Existem algumas implementações, como o Suite B da NSA. Entretanto, a maioria delas possuem patentes

Privacidade em Smart Metering por Borges et al. (iKUP)

1- Cada medidor possui:

- Uma chave simétrica $\boldsymbol{d_i}$
- Uma chave privada $\boldsymbol{k_i}$
- As chaves públicas dos vizinhos (ex., $\boldsymbol{p_{i-1}}$ e $\boldsymbol{p_{i+1}}$)
- Uma função hash $\boldsymbol{H}$
- Assume-se que a concessionária possui a lista de chaves simétricas $\boldsymbol{\{d_1, d_2, \ldots, d_n\}}$

Privacidade em Smart Metering por Borges et al. (iKUP)

SM_1

d_1, k_1, p_2, H

Medidores formam uma spanning tree

SM_2

d_2, k_2, p_1, p_3, H

MDM

$\{d_1, d_2, \ldots, d_n\}$

...

SM_N

d_N, k_N, p_{N-1}, H

Privacidade em Smart Metering por Borges et al. (iKUP)

2- O medidor $\boldsymbol{SM_1}$ calcula a sua medição $\boldsymbol{m_1}$, e para um instante de tempo $\boldsymbol{t}$ computa:
$\boldsymbol{c_1 = m_1 + H(d_1 \parallel t)}$. Em seguida, ele envia $\boldsymbol{c_1}$ criptografado com $\boldsymbol{p_2}$ para $\boldsymbol{SM_2}$

- SM2 então computa $\boldsymbol{c_2 = c1 + m_2 + H(d_2 \parallel t) = m_1 + H(d_1 \parallel t) + m_2 + H(d_2 \parallel t)}$, criptografa com $\boldsymbol{p_3}$ e envia para $\boldsymbol{SM_3}$
- Este processo continua até $\boldsymbol{SM_N}$, que por fim, envia $\boldsymbol{c_n}$ para a concessionária

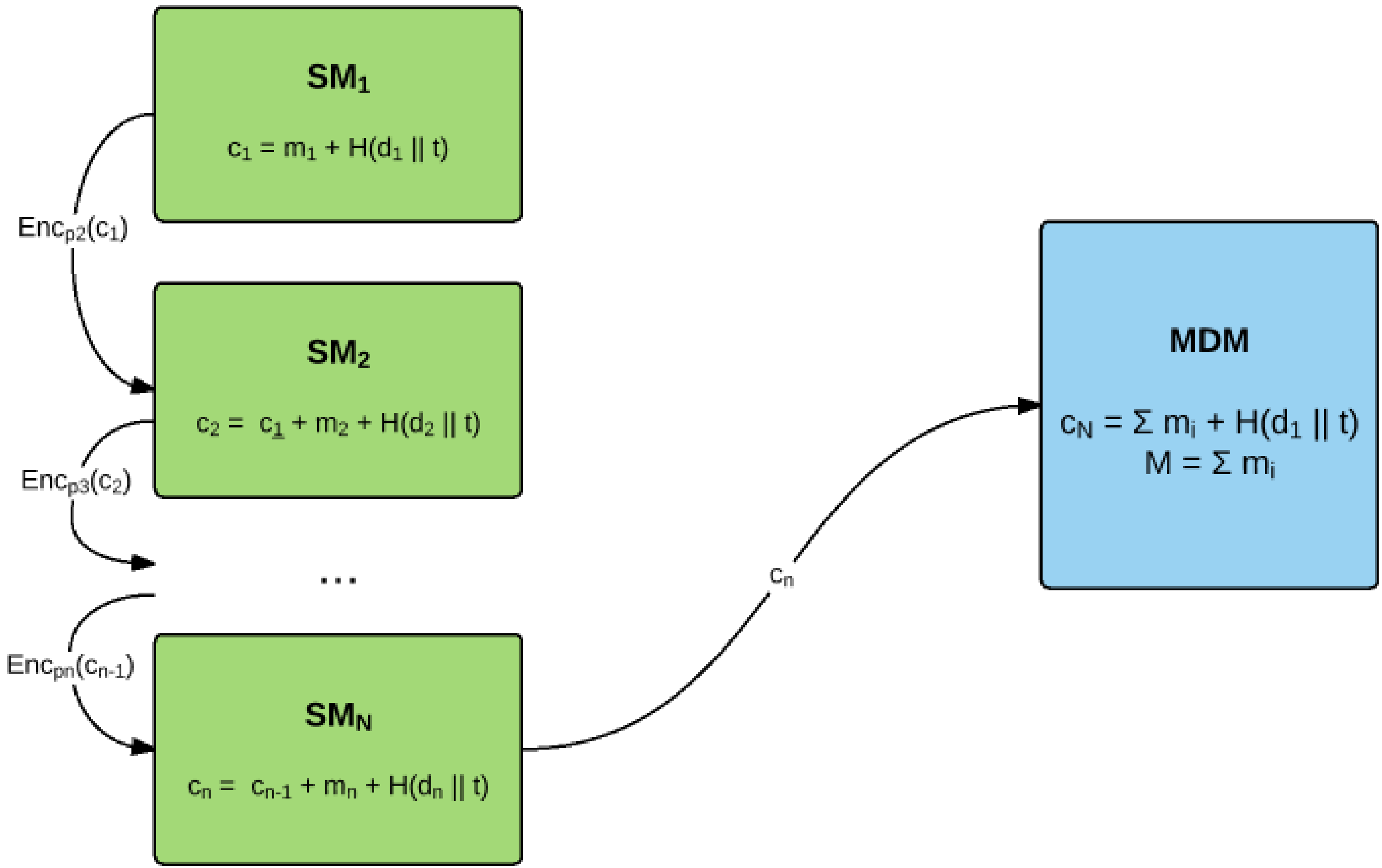
Privacidade em Smart Metering por Borges et al. (iKUP)

3- A concessionária obtém do último medidor

$$c_N = \Sigma\, m_i + H(d_1 \,||\, t)$$

– Como ela possui $\{d_1, d_2, \ldots, d_n\}$ e sabe os timestamps, ela consegue obter $M = \Sigma m_i$

Privacidade em Smart Metering por Borges et al.



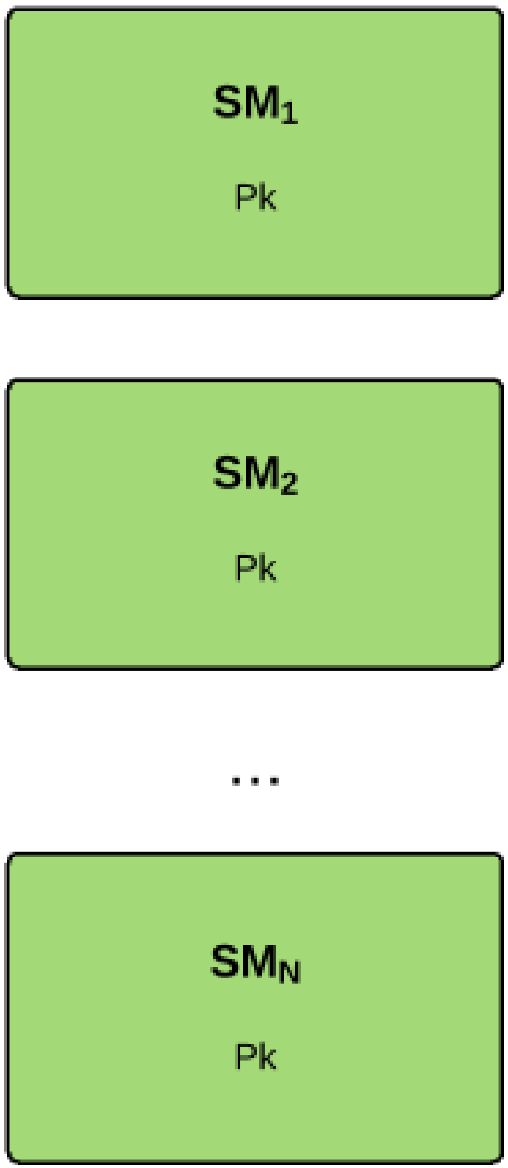
Privacidade em Smart Metering por Borges et al. (Usando Paillier)

1- Cada medidor possui:

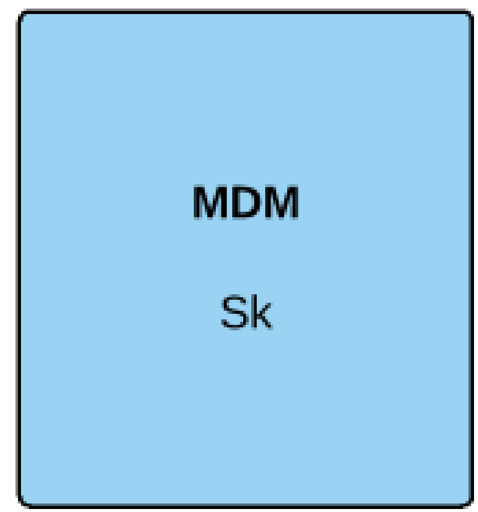
- As chaves públicas dos vizinhos (ex., $\boldsymbol{p_{i-1}}$ e $\boldsymbol{p_{i+1}}$)
- A chave pública de Paillier da concessionária ($\mathbf{P_k}$)

- A concessionária possui uma chave privada de Paillier ($\mathbf{S_k}$)

Privacidade em Smart Metering por Borges et al. (Usando Paillier)



Medidores formam uma spanning tree



Privacidade em Smart Metering por Borges et al. (Usando Paillier)

2- O medidor $\boldsymbol{SM_1}$ calcula a sua medição $\boldsymbol{m_1}$, e para um instante de tempo $\boldsymbol{t}$ computa:
$\boldsymbol{c_1 = Enc_{Pk}(m_1)}$. Em seguida, ele envia $\boldsymbol{c_1}$ para $\boldsymbol{SM_2}$

- SM2 então computa $\boldsymbol{Enc_{Pk}(m_2)}$ e $\boldsymbol{c_2 = c1 \cdot Enc_{Pk}(m_2)}$, e envia para $\boldsymbol{SM_3}$
- Este processo continua até $\boldsymbol{SM_N}$, que por fim, envia $\boldsymbol{c_n}$ para a concessionária

Privacidade em Smart Metering por Borges et al. (Usando Paillier)

3- Devido a propriedade homomorfica de Paillier concessionária obtém do último medidor

$\boldsymbol{c_N = Enc_{Pk}(\Sigma\ m_i)}$

– Ao descriptografar, ela obtém $\boldsymbol{M = \Sigma m_i}$

Privacidade em Smart Metering por Borges et al. (Usando Paillier)