Criptografie și Securitate

- Prelegerea 22.2 -
Sistemul de criptare ElGamal pe curbe eliptice

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

Sistemul de criptare ElGamal pe curbe eliptice

- Am studiat sistemul de criptare ElGamal peste un grup ciclic $\mathbb{G}$, de ordin q;

Sistemul de criptare ElGamal pe curbe eliptice

- Am studiat sistemul de criptare ElGamal peste un grup ciclic $\mathbb{G}$, de ordin q;
- Transpunem construcția pe curbe eliptice:

$$(\mathbb{G}, \cdot) \to (E(\mathbb{Z}_q), +)$$

Sistemul de criptare ElGamal pe curbe eliptice

1. Se generează $E(\mathbb{Z}_q)$ o curbă eliptică și P un punct pe curbă (generator), se alege $x \leftarrow^R \mathbb{Z}_q$ și se calculează $H = xP$;
   - Cheia publică este: $(E(\mathbb{Z}_q), P, H)$;
   - Cheia privată este $(E(\mathbb{Z}_q), P, x)$;

2. **Enc**: dată o cheie publică $(E(\mathbb{Z}_q), P, H)$ și un mesaj $M \in E(\mathbb{Z}_q)$, alege $y \leftarrow^R \mathbb{Z}_q$ și întoarce $C = (C_1, C_2) = (yP, M + yH)$;

3. **Dec**: dată o cheie secretă $(E(\mathbb{Z}_q), P, x)$ și un mesaj criptat $C = (C_1, C_2)$, întoarce $M = C_2 + x(-C_1)$.

Securitate

- Sistemul transpus pe curbe eliptice păstează proprietățile sistemului inițial;
- Deci curba eliptică trebuie aleasă a.î. ECDLP și ECDDH să fie dificile...

Securitate

- Sistemul transpus pe curbe eliptice păstează proprietățile sistemului inițial;
- Deci curba eliptică trebuie aleasă a.î. ECDLP și ECDDH să fie dificile...
- ... și sistemul rămâne nedeterminist și homomorfic.

Important de reținut!

- Sistemul de criptare ElGamal pe curbe eliptice