Securitatea Sistemelor Informatice

- Curs 12 -
Criptografia post-cuantică

Adela Georgescu

Facultatea de Matematică și Informatică
Universitatea din București
Anul universitar 2022-2023, semestrul I

Criptografia post-cuantică

- In cadrul criptografiei de până acum am discutat despre un adversar PPT care rulează în timp polinomial pe un *calculator convențional (clasic)*. In evaluarea securității primitvelor criptografie am considerat numai *atacuri clasice*.

Criptografia post-cuantică

- In cadrul criptografiei de până acum am discutat despre un adversar PPT care rulează în timp polinomial pe un *calculator convențional (clasic)*. In evaluarea securității primitvelor criptografie am considerat numai *atacuri clasice*.
- Nu am avut in vedere *calculatoarele cuantice* - care se bazează pe principiile mecanicii cuantice și impactul lor asupra securității

Criptografia post-cuantică

- In cadrul criptografiei de până acum am discutat despre un adversar PPT care rulează în timp polinomial pe un *calculator convențional (clasic)*. In evaluarea securității primitvelor criptografie am considerat numai *atacuri clasice*.
- Nu am avut in vedere *calculatoarele cuantice* - care se bazează pe principiile mecanicii cuantice și impactul lor asupra securității
- Algoritmii cuantici pot fi, în anumite cazuri, mult mai rapizi decât cei clasici și pot avea un impact zdrobitor asupra securității primitivelor criptografice studiate.

Criptografia post-cuantică

- D.p.d.v. teoretic, impactul calculatoarelor cuantice asupra criptografiei este recunoscut din anii 1990.

Criptografia post-cuantică

- D.p.d.v. teoretic, impactul calculatoarelor cuantice asupra criptografiei este recunoscut din anii 1990.

- Practic, un calculator cuantic generic, pe scară largă nu există iar costurile pentru construcția lui ar fi uriașe

Criptografia post-cuantică

- D.p.d.v. teoretic, impactul calculatoarelor cuantice asupra criptografiei este recunoscut din anii 1990.
- Practic, un calculator cuantic generic, pe scară largă nu există iar costurile pentru construcția lui ar fi uriașe
- Totusi, un calculator cuantic dedicat care să atace sistemele de criptare actuale ar putea apărea în decurs de câtiva ani sau zeci de ani.

Criptografia post-cuantică

- D.p.d.v. teoretic, impactul calculatoarelor cuantice asupra criptografiei este recunoscut din anii 1990.
- Practic, un calculator cuantic generic, pe scară largă nu există iar costurile pentru construcția lui ar fi uriașe
- Totusi, un calculator cuantic dedicat care să atace sistemele de criptare actuale ar putea apărea în decurs de câtiva ani sau zeci de ani.
- Odată ce un astfel de calculator cuantic care să poate fi folosit în practică devine disponibil, toți algoritmii cu cheie publică folosiți în prezent dar și protocoalele asociate devin vulnerabile

Criptografia post-cuantică

- D.p.d.v. teoretic, impactul calculatoarelor cuantice asupra criptografiei este recunoscut din anii 1990.
- Practic, un calculator cuantic generic, pe scară largă nu există iar costurile pentru construcția lui ar fi uriașe
- Totusi, un calculator cuantic dedicat care să atace sistemele de criptare actuale ar putea apărea în decurs de câtiva ani sau zeci de ani.
- Odată ce un astfel de calculator cuantic care să poate fi folosit în practică devine disponibil, toți algoritmii cu cheie publică folosiți în prezent dar și protocoalele asociate devin vulnerabile
- Aceasta înseamnă că toate email-urile, informațiile despre cardurile cu care facem plăți online, semnături digitale, tranzacții online, datele sensibile, informațiile clasificate ale agențiilor de securitate și cele guvernamentale vor fi în pericol

Competiția NIST pentru standardizare post-cuantică

- Ca urmare, NIST a lansat în 2017 o competiție (încă în desfășurare) pentru evaluarea și standardizarea unor scheme (de criptare, de semnatura) cu cheie publică post-cuantice - care rămân sigure în fata unor algoritmi cuantici polinomiali. `https://csrc.nist.gov/projects/post-quantum-cryptography`.
- Competitia a fost lansată în 2017 și in prima runda au fost acceptate 69 de propuneri (din cele 82 primite) https://csrc.nist.gov/Projects/post-quantum-cryptography

Competiția NIST pentru standardizare post-cuantică

- Ca urmare, NIST a lansat în 2017 o competiție (încă în desfășurare) pentru evaluarea și standardizarea unor scheme (de criptare, de semnatura) cu cheie publică post-cuantice - care rămân sigure în fata unor algoritmi cuantici polinomiali. `https://csrc.nist.gov/projects/post-quantum-cryptography`.
- Competitia a fost lansată în 2017 și in prima runda au fost acceptate 69 de propuneri (din cele 82 primite) https://csrc.nist.gov/Projects/post-quantum-cryptography
- La începutul lui 2019, au fost aleși 26 de candidați pentru runda a 2-a.

Competiția NIST pentru standardizare post-cuantică

- Ca urmare, NIST a lansat în 2017 o competiție (încă în desfășurare) pentru evaluarea și standardizarea unor scheme (de criptare, de semnatura) cu cheie publică post-cuantice - care rămân sigure în fata unor algoritmi cuantici polinomiali. `https://csrc.nist.gov/projects/post-quantum-cryptography`.
- Competitia a fost lansată în 2017 și in prima runda au fost acceptate 69 de propuneri (din cele 82 primite) https://csrc.nist.gov/Projects/post-quantum-cryptography
- La începutul lui 2019, au fost aleși 26 de candidați pentru runda a 2-a.
- Iulie 2020 - anuntați pentru runda a 3-a: 7 finaliști și 8 candidati alternativi

Competiția NIST pentru standardizare post-cuantică

- Iulie 2022 - NIST anunță primul grup de 4 finaliști

Competiția NIST pentru standardizare post-cuantică

- Iulie 2022 - NIST anunță primul grup de 4 finaliști
  - **criptare**: CRYSTALS - Kyber - pentru chei mici de criptare și operații rapide

Competiția NIST pentru standardizare post-cuantică

- Iulie 2022 - NIST anunță primul grup de 4 finaliști
  - **criptare**: CRYSTALS - Kyber - pentru chei mici de criptare și operații rapide
  - **semnături digitale**
    - CRYSTALS-Dilithium
    - FALCON
    - SPHINCS+
- Dilithium și Falcon sunt foarte eficienți, cel din urmă fiind recomandat atunci când sunt necesare semnături mai mici decât cele oferite de Dilithium

Competiția NIST pentru standardizare post-cuantică

- Iulie 2022 - NIST anunță primul grup de 4 finaliști
  - **criptare**: CRYSTALS - Kyber - pentru chei mici de criptare și operații rapide
  - **semnături digitale**
    - CRYSTALS-Dilithium
    - FALCON
    - SPHINCS+
- Dilithium și Falcon sunt foarte eficienți, cel din urmă fiind recomandat atunci când sunt necesare semnături mai mici decât cele oferite de Dilithium
- Primii 3 algoritmi se bazează pe probleme matematice de latici, iar SPHINCS+ folosește funcții hash

Competiția NIST pentru standardizare post-cuantică

- Iulie 2022 - NIST anunță primul grup de 4 finaliști
  - **criptare**: CRYSTALS - Kyber - pentru chei mici de criptare și operații rapide
  - **semnături digitale**
    - CRYSTALS-Dilithium
    - FALCON
    - SPHINCS+
- Dilithium și Falcon sunt foarte eficienți, cel din urmă fiind recomandat atunci când sunt necesare semnături mai mici decât cele oferite de Dilithium
- Primii 3 algoritmi se bazează pe probleme matematice de latici, iar SPHINCS+ folosește funcții hash
- Procesul de standardizare se va finaliza în anul 2024

Competiția NIST pentru standardizare post-cuantică

- Iulie 2022 - NIST anunță primul grup de 4 finaliști
  - **criptare**: CRYSTALS - Kyber - pentru chei mici de criptare și operații rapide
  - **semnături digitale**
    - CRYSTALS-Dilithium
    - FALCON
    - SPHINCS+
- Dilithium și Falcon sunt foarte eficienți, cel din urmă fiind recomandat atunci când sunt necesare semnături mai mici decât cele oferite de Dilithium
- Primii 3 algoritmi se bazează pe probleme matematice de latici, iar SPHINCS+ folosește funcții hash
- Procesul de standardizare se va finaliza în anul 2024
- Alți 4 algoritmi sunt considerați pentru standardizare

Criptografia post-cuantică vs. criptografia cuantică

Criptografia cuantică

- implementări folosind calculatoare cuantice, fenomene mecanice cuantice și canale de comunicare cuantice
- dificil de implementat la scara largă
- în unele cazuri este sigură necondiționat (nu se bazează pe ipoteze matematice)

Criptografia post-cuantică

- implementări folosind calculatoare clasice
- este sigură chiar și în fața unui adversar care are acces la un calculator cuantic
- se bazează pe probleme matematice dificile computațional chiar și pentru algoritmii cuantici

Criptografia simetrică post-cuantică

- Impactul calculatoarelor cuantice asupra criptografiei simetrice este minor; ilustram pe scurt

Criptografia simetrică post-cuantică

- Impactul calculatoarelor cuantice asupra criptografiei simetrice este minor; ilustram pe scurt
- Considerăm următoarea problema abstractă:

Criptografia simetrică post-cuantică

- Impactul calculatoarelor cuantice asupra criptografiei simetrice este minor; ilustram pe scurt
- Considerăm următoarea problema abstractă:
  - Se dă: funcție $f : D \to \{0, 1\}$ cu acces de tip oracol (funcția poate fi interogată pe orice input și se primește output-ul corespunzător)

Criptografia simetrică post-cuantică

- Impactul calculatoarelor cuantice asupra criptografiei simetrice este minor; ilustram pe scurt
- Considerăm următoarea problema abstractă:
  - Se dă: funcție $f : D \to \{0, 1\}$ cu acces de tip oracol (funcția poate fi interogată pe orice input și se primește output-ul corespunzător)
  - Se cere: să se găsească x a.î. $f(x) = 1$.

Criptografia simetrică post-cuantică

- Impactul calculatoarelor cuantice asupra criptografiei simetrice este minor; ilustram pe scurt
- Considerăm următoarea problema abstractă:
  - Se dă: funcție $f : D \rightarrow \{0, 1\}$ cu acces de tip oracol (funcția poate fi interogată pe orice input și se primește output-ul corespunzător)
  - Se cere: să se găsească x a.î. $f(x) = 1$.
- Dacă există un singur x cu $f(x) = 1$ atunci orice algoritm clasic necesită $\mathrm{O}(\|D\|)$ evaluări ale funcției f - corespunde unui atac prin forță brută
- 1996 - algoritmul cuantic al lui Grover: găsește x folosind $\mathrm{O}(\|D^{1/2}\|)$ evaluări ale funcției f. Algorimtul este optim, și nu poate fi îmbunătățit

Criptografia simetrică post-cuantică - sisteme bloc

- Trecem in revista impactul algoritmului asupra sistemelor de criptare simetrice

Criptografia simetrică post-cuantică - sisteme bloc

- Trecem in revista impactul algoritmului asupra sistemelor de criptare simetrice
- Considerăm cazul unui sistem de criptare bloc $F : \{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^l$ cu cheia k pe n biți pentru care cel mai bun atac (de găsire a cheii) este forța brută.

Criptografia simetrică post-cuantică - sisteme bloc

- Trecem in revista impactul algoritmului asupra sistemelor de criptare simetrice
- Considerăm cazul unui sistem de criptare bloc $F : \{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^l$ cu cheia k pe n biți pentru care cel mai bun atac (de găsire a cheii) este forța brută.
- Un astfel de atac clasic necesită timp 2^n

Criptografia simetrică post-cuantică - sisteme bloc

- Trecem in revista impactul algoritmului asupra sistemelor de criptare simetrice
- Considerăm cazul unui sistem de criptare bloc $F : \{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^l$ cu cheia k pe n biți pentru care cel mai bun atac (de găsire a cheii) este forța brută.
- Un astfel de atac clasic necesită timp 2^n
- Pentru securitate, alegem cheia k de lungime n biti așa încât timpul pentru atac 2^n să nu fie practic

Criptografia simetrică post-cuantică - sisteme bloc

- Trecem in revista impactul algoritmului asupra sistemelor de criptare simetrice
- Considerăm cazul unui sistem de criptare bloc $F : \{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^l$ cu cheia k pe n biți pentru care cel mai bun atac (de găsire a cheii) este forța brută.
- Un astfel de atac clasic necesită timp 2^n
- Pentru securitate, alegem cheia k de lungime n biti așa încât timpul pentru atac 2^n să nu fie practic
- Algoritmul lui Grover însă permite unui atacator să găsească cheia în timp $2^{n/2}$.

Criptografia simetrică post-cuantică - sisteme bloc

- Trecem in revista impactul algoritmului asupra sistemelor de criptare simetrice
- Considerăm cazul unui sistem de criptare bloc $F : \{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^l$ cu cheia k pe n biți pentru care cel mai bun atac (de găsire a cheii) este forța brută.
- Un astfel de atac clasic necesită timp 2^n
- Pentru securitate, alegem cheia k de lungime n biti așa încât timpul pentru atac 2^n să nu fie practic
- Algoritmul lui Grover însă permite unui atacator să găsească cheia în timp $2^{n/2}$.
- Pentru același nivel de securitate (precum în cazul clasic), alegem cheia k de lungime **dublă** fața de cazul clasic.

Criptografia simetrică post-cuantică - funcții hash

- Considerăm problema găsirii de coliziuni pentru o funcție hash $H : \{0,1\}^m \rightarrow \{0,1\}^n$ cu $m > n$.

Criptografia simetrică post-cuantică - funcții hash

- Considerăm problema găsirii de coliziuni pentru o funcție hash $H : \{0,1\}^m \rightarrow \{0,1\}^n$ cu $m > n$.
- In cazul **clasic**, am văzut că "atacul nașterilor" necesită $O(2^{n/2})$ evaluări ale funcției H.

Criptografia simetrică post-cuantică - funcții hash

- Considerăm problema găsirii de coliziuni pentru o funcție hash $H : \{0, 1\}^m \to \{0, 1\}^n$ cu $m > n$.
- In cazul **clasic**, am văzut că "atacul nașterilor" necesită $O(2^{n/2})$ evaluări ale funcției H.
- Aceasta înseamnă că pentru a asigura rezistența la coliziuni fața de un atac în timp 2^t, trebuie să alegem funcții hash cu output-ul pe $2t$ biți.

Criptografia simetrică post-cuantică - funcții hash

- Considerăm problema găsirii de coliziuni pentru o funcție hash $H : \{0,1\}^m \to \{0,1\}^n$ cu $m > n$.
- In cazul **clasic**, am văzut că "atacul nașterilor" necesită $O(2^{n/2})$ evaluări ale funcției H.
- Aceasta înseamnă că pentru a asigura rezistența la coliziuni fața de un atac în timp 2^t, trebuie să alegem funcții hash cu output-ul pe $2t$ biți.
- Insă în cazul **cuantic**, un atac pentru găsirea coliziunilor necesită $O(2^{n/3})$ evaluări ale funcției H.

Criptografia simetrică post-cuantică - funcții hash

- Considerăm problema găsirii de coliziuni pentru o funcție hash $H : \{0,1\}^m \rightarrow \{0,1\}^n$ cu $m > n$.
- In cazul **clasic**, am văzut că "atacul naşterilor" necesită $O(2^{n/2})$ evaluări ale funcției H.
- Aceasta înseamnă că pentru a asigura rezistența la coliziuni fața de un atac în timp 2^t, trebuie să alegem funcții hash cu output-ul pe $2t$ biți.
- Insă în cazul **cuantic**, un atac pentru găsirea coliziunilor necesită $O(2^{n/3})$ evaluări ale funcției H.
- Deci, pentru a asigura rezistența la coliziuni față de un atac în timp 2^t, trebuie să alegem funcții hash cu output-ul pe $3t$ biți.

Algoritmul lui Shor și impactul lui asupra criptografiei asimetrice

- Până acum am văzut algoritmi cuantici care oferă o îmbunătățire de *ordin polinomial* în comparație cu cei mai buni algoritmi clasici pentru aceeași problemă.

Algoritmul lui Shor și impactul lui asupra criptografiei asimetrice

- Până acum am văzut algoritmi cuantici care oferă o îmbunătățire de *ordin polinomial* în comparație cu cei mai buni algoritmi clasici pentru aceeași problemă.
- Aceștia impun doar creșterea dimensiunilor cheilor fără a necesita alte schimbari majore

Algoritmul lui Shor și impactul lui asupra criptografiei asimetrice

- Până acum am văzut algoritmi cuantici care oferă o îmbunătățire de *ordin polinomial* în comparație cu cei mai buni algoritmi clasici pentru aceeași problemă.
- Aceștia impun doar creșterea dimensiunilor cheilor fără a necesita alte schimbari majore
- In continuare vom vedea un algoritm care oferă o îmbunătățire de *ordin exponențial* - **algoritmi cuantici polinomiali pentru problema factorizarii și problema logaritmului discret**

Algoritmul lui Shor și impactul lui asupra criptografiei asimetrice

- Incepem cu o problemă abstractă:
  - Se dă: o funcție $f : \mathbb{G} \to R$, cu $\mathbb{G}$ un grup comutativ.
  - Presupunem f *periodică*: există $\alpha \in \mathbb{G}$ - *perioadă*- cu $f(x) = f(x + \alpha)$
  - Se cere: găsirea unei perioade având acces de tip oracol la funcția f

Algoritmul lui Shor și impactul lui asupra criptografiei asimetrice

- Incepem cu o problemă abstractă:
  - Se dă: o funcție $f : \mathbb{G} \to R$, cu $\mathbb{G}$ un grup comutativ.
  - Presupunem f *periodică*: există $\alpha \in \mathbb{G}$ - *perioadă*- cu $f(x) = f(x + \alpha)$
  - Se cere: găsirea unei perioade având acces de tip oracol la funcția f
- Nu se cunosc algoritmi clasici eficienți pentru rezolvarea acestei probleme.

Algoritmul lui Shor și impactul lui asupra criptografiei asimetrice

- 1994 - Shor - rezultat uimitor: *algoritm cuantic polinomial* care rezolvă problema pentru anumite grupuri $\mathbb{G}$.
- Este un instrument puternic care poate fi folosit pentru a factoriza și a calcula logaritmi discreti.
- Trebuie doar aleasă cu grijă funcția a cărei perioadă ne dă soluția pe care o căutăm

Algoritmul lui Shor și impactul lui asupra factorizarii

- Considerăm problema factorizarii: fie N un produs de două numere prime. Pentru orice $x \in \mathbb{Z}_N^*$, definim funcția $f_{x,N} : \mathbb{Z} \to \mathbb{Z}_N^*$

$$f_{x,N}(r) = x^r \bmod N$$

- Principala observație este că funcția are perioada $\phi(N)$ deoarece

$$f_{x,N}(r+\phi(N)) = x^{r+\phi(N)} \bmod N = x^r \cdot x^{\phi(N)} \bmod N = x^r \bmod N$$

- Pentru orice x ales de noi, putem calcula, in timp polinomial, cu algoritmul lui Shor, o perioadă a funcției $f_{x,N}$ adică un $k \neq 0$ cu $x^k = 1 \bmod N$. Aceasta imediat permite factorizarea lui N în timp polinomial.

Algoritmul lui Shor și impactul lui asupra criptografiei asimetrice

- Algoritmul lui Shor poate fi folosit și pentru rezolvarea problemei logaritmului discret în timp polinomial
- Având în vedere că toate sistemele de criptare cu cheie publică se bazează pe problema factorizării sau problema logaritmului discret, concluzionăm că

  Toate sistemele de criptare cu cheie publică prezentate la curs pot fi atacate în timp polinomial cu ajutorul unui calculator cuantic

Sisteme de criptare cu cheie publică post-cuantice

- Problema factorizării și problema logaritmului discret devin "ușoare" pentru un calculator cuantic.

Sisteme de criptare cu cheie publică post-cuantice

- Problema factorizării și problema logaritmului discret devin "ușoare" pentru un calculator cuantic.

- Avem nevoie de probleme matematice dificile computațional chiar și pentru calculatoarele cuantice, dar care rulează pe calculatoare clasice

Sisteme de criptare cu cheie publică post-cuantice

- Problema factorizării și problema logaritmului discret devin "ușoare" pentru un calculator cuantic.
- Avem nevoie de probleme matematice dificile computațional chiar și pentru calculatoarele cuantice, dar care rulează pe calculatoare clasice
- Diferenta față de cazul clasic este că problemele considerate pentru criptografia post-cuantică sunt mai recente și nu au fost studiate la fel de mult ca problema factorizării sau problema logaritmului discret

Sisteme de criptare cu cheie publică post-cuantice

- Problema factorizării și problema logaritmului discret devin "ușoare" pentru un calculator cuantic.
- Avem nevoie de probleme matematice dificile computațional chiar și pentru calculatoarele cuantice, dar care rulează pe calculatoare clasice
- Diferenta față de cazul clasic este că problemele considerate pentru criptografia post-cuantică sunt mai recente și nu au fost studiate la fel de mult ca problema factorizării sau problema logaritmului discret
- In continuare vom prezenta o problemă care a primit multa atenție și care este considerată dificilă chiar și pentru calculatoarele cuantice. Aratam apoi cum se poate construi un sistem de criptare cu cheie publica bazat pe dificultatea acelei probleme.

Problema LWE - Learning With Errors

- A fost introdusa in 2005 de Oded Regev

Problema LWE - Learning With Errors

- A fost introdusa in 2005 de Oded Regev
- Preliminarii:
  - q număr prim. Vom nota cu $\mathbb{Z}_q$ mulțimea $\{-\lfloor (q-1)/2 \rfloor, ..., 0, ..., \lfloor q/2 \rfloor\}$ (spre deosebire de $\{0, ..., q\}$) unde $\lfloor x \rfloor$ este cel mai mare intreg mai mic sau egal cu x.
  - spunem că un element al lui $\mathbb{Z}_q$ este "mic" dacă este "aproape" de 0.

Problema LWE - Learning With Errors

- A fost introdusa in 2005 de Oded Regev

- Preliminarii:
  - q număr prim. Vom nota cu $\mathbb{Z}_q$ mulțimea $\{-\lfloor (q-1)/2 \rfloor, ..., 0, ..., \lfloor q/2 \rfloor\}$ (spre deosebire de $\{0, ..., q\}$) unde $\lfloor x \rfloor$ este cel mai mare intreg mai mic sau egal cu x.
  - spunem că un element al lui $\mathbb{Z}_q$ este "mic" dacă este "aproape" de 0.

- Problema cere găsirea lui $\mathbf{s} \in \mathbb{Z}_q^n$ fiind dată o secvență de ecuații liniare "aproximative" în $\mathbf{s}$.

Problema LWE - Learning With Errors

- A fost introdusa in 2005 de Oded Regev
- Preliminarii:
  - q număr prim. Vom nota cu $\mathbb{Z}_q$ mulțimea $\{-\lfloor (q-1)/2 \rfloor, ..., 0, ..., \lfloor q/2 \rfloor\}$ (spre deosebire de $\{0, ..., q\}$) unde $\lfloor x \rfloor$ este cel mai mare intreg mai mic sau egal cu x.
  - spunem că un element al lui $\mathbb{Z}_q$ este "mic" dacă este "aproape" de 0.
- Problema cere găsirea lui $\mathbf{s} \in \mathbb{Z}_q^n$ fiind dată o secvență de ecuații liniare "aproximative" în $\mathbf{s}$.
- Exemplu:

$$
\begin{aligned}
12s_1 + 10s_2 + 5s_3 + 2s_4 &\approx 8 \text{ mod } 17 \\
3s_1 + 7s_2 + 9s_3 + s_4 &\approx 4 \text{ mod } 17 \\
16s_1 + 2s_2 + 8s_3 + 7s_4 &\approx 3 \text{ mod } 17
\end{aligned}
$$

Problema LWE - Learning With Errors

- Exemplul

$$\begin{aligned} 12s_1 + 10s_2 + 5s_3 + 2s_4 + 1 &= 8 \bmod 17 \\ 3s_1 + 7s_2 + 9s_3 + s_4 - 1 &= 4 \bmod 17 \\ 16s_1 + 2s_2 + 8s_3 + 7s_4 + 2 &= 3 \bmod 17 \end{aligned}$$

sub forma matriciala

$$\begin{bmatrix} 12 & 10 & 5 & 2 \\ 3 & 7 & 9 & 1 \\ 16 & 2 & 8 & 7 \end{bmatrix} * \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix} \approx \begin{bmatrix} 8 \\ 4 \\ 3 \end{bmatrix}$$

sau, notand matricile corespunzator (unde $\mathbf{s} = (s_1, s_2, s_3)$), ecuația matricială devine

$$\mathbf{As} + \mathbf{e} = \mathbf{b} \bmod q$$

Problema LWE - Learning With Errors

$$\begin{pmatrix} 12 & 10 & 5 & 2 \\ 3 & 7 & 9 & 1 \\ 16 & 2 & 8 & 7 \end{pmatrix} * \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} \approx \begin{pmatrix} 8 \\ 4 \\ 3 \end{pmatrix}$$

- vectorul $\mathbf{e} = (1, -1, 2)$ este format din elemente "mici" din $\mathbb{Z}$ numite *noise* sau *error*.

Problema LWE - Learning With Errors

$$\begin{bmatrix} 12 & 10 & 5 & 2 \\ 3 & 7 & 9 & 1 \\ 16 & 2 & 8 & 7 \end{bmatrix} * \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix} \approx \begin{bmatrix} 8 \\ 4 \\ 3 \end{bmatrix}$$

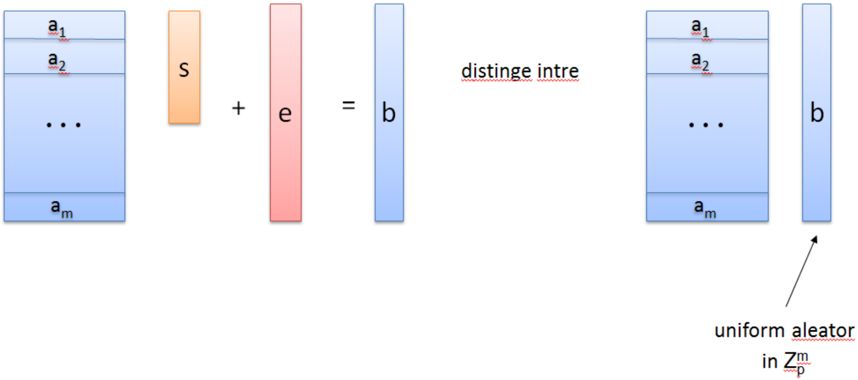
- vectorul $\mathbf{e} = (1, -1, 2)$ este format din elemente "mici" din $\mathbb{Z}$ numite *noise* sau *error*.
- In lipsa lui **e**, ecuația $\mathbf{As} = \mathbf{b}$ devine usor de rezolvat cu tehnici clasice de algebra liniară

Problema LWE - Learning With Errors

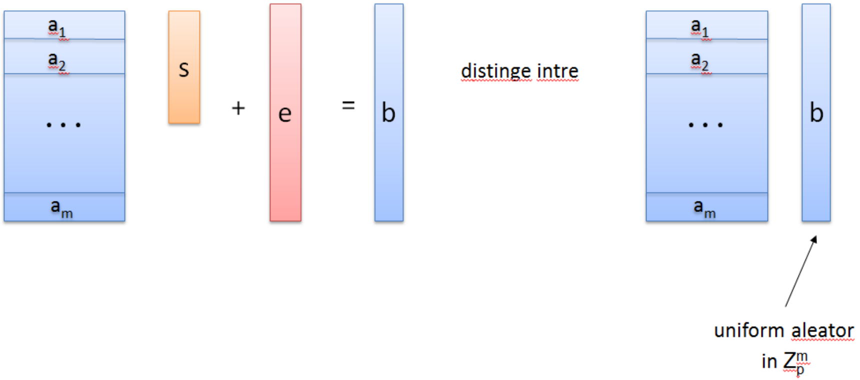
$$\begin{pmatrix} 12 & 10 & 5 & 2 \\ 3 & 7 & 9 & 1 \\ 16 & 2 & 8 & 7 \end{pmatrix} * \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} \approx \begin{pmatrix} 8 \\ 4 \\ 3 \end{pmatrix}$$

- vectorul $\mathbf{e} = (1, -1, 2)$ este format din elemente "mici" din $\mathbb{Z}$ numite *noise* sau *error*.
- In lipsa lui $\mathbf{e}$, ecuația $\mathbf{As} = \mathbf{b}$ devine usor de rezolvat cu tehnici clasice de algebra liniară
- Cand matricea **A** are suficient de multe linii și parametrii sunt aleși corespunzător, problema devine dificilă.

Problema decizională LWE



Problema decizională LWE



- Problema decizională cere să se distingă între un **b** generat ca mai sus (stânga) și un **b** generat uniform aleator în $\mathbb{Z}_q^m$.

Sistem de criptare bazat pe LWE

Descriem mai întâi un schimb de chei (nesigur) care poate fi văzut ca o versiune algebric liniară a schimbului de chei Diffie-Hellman. Fixează parametrii $n, q, \chi, m > n$


Alice


Bob

Alice		Bob
$\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times n}, \mathbf{s} \leftarrow \chi^n$	$\xrightarrow{\mathbf{A},\, t_A}$	$\bar{\mathbf{s}} \leftarrow \chi^m$
$t_A := \mathbf{A} \cdot \mathbf{s} \bmod q$	$\xleftarrow{t_B^T}$	$t_B^T := \bar{\mathbf{s}}^T \cdot \mathbf{A} \bmod q$
$k_A := t_B^T \cdot \mathbf{s} \bmod q$		$k_B := \bar{\mathbf{s}}^T \cdot t_A \bmod q$

- Verificăm ușor că Alice și Bob partajează aceeași cheie $k_A := t_B^T \cdot \mathbf{s} = \bar{\mathbf{s}}^T \cdot \mathbf{A} \cdot \mathbf{s} = \bar{\mathbf{s}}^T \cdot t_A = k_B$

Sistem de criptare bazat pe LWE

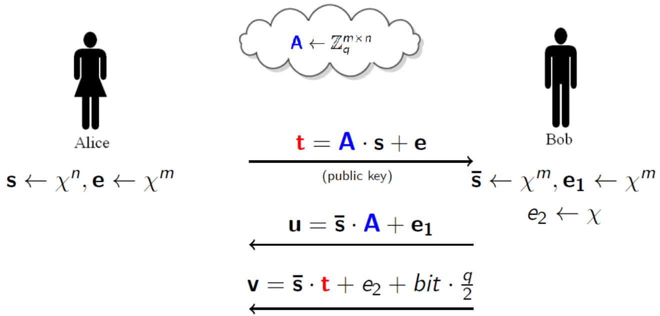
- Protocolul de mai sus nu este sigur pentru că un atacator poate calcula $\bar{\mathbf{s}}$ sau $\mathbf{s}$ cu noțiuni de algebră liniară și poate afla și cheia.

Sistem de criptare bazat pe LWE

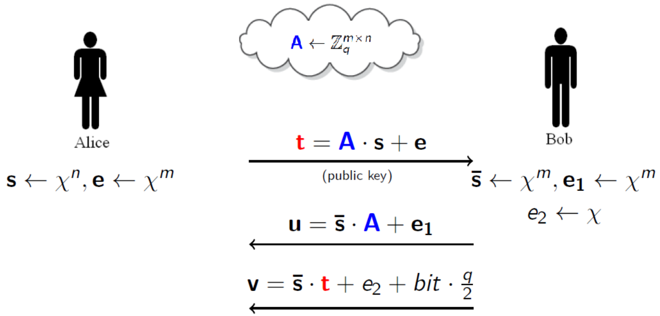
- Protocolul de mai sus nu este sigur pentru că un atacator poate calcula $\bar{\mathbf{s}}$ sau $\mathbf{s}$ cu noțiuni de algebră liniară și poate afla și cheia.
- Insă el poate fi transformat într-un protocol sigur și adaptat ca un sistem de criptare adăugând "noise", sub ipoteza problemei decizionale LWE.

Sistem de criptare bazat pe LWE

- Protocolul de mai sus nu este sigur pentru că un atacator poate calcula $\bar{\mathbf{s}}$ sau $\mathbf{s}$ cu noțiuni de algebră liniară și poate afla și cheia.
- Insă el poate fi transformat într-un protocol sigur și adaptat ca un sistem de criptare adăugând "noise", sub ipoteza problemei decizionale LWE.

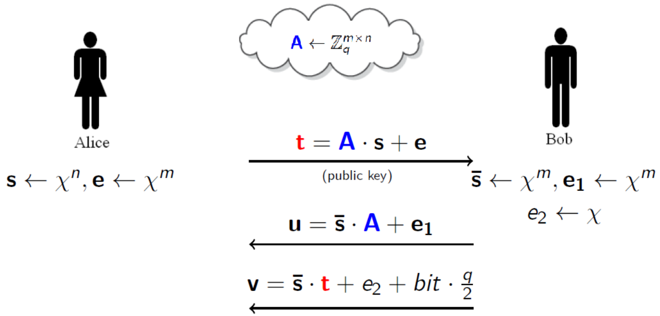


Sistem de criptare bazat pe LWE



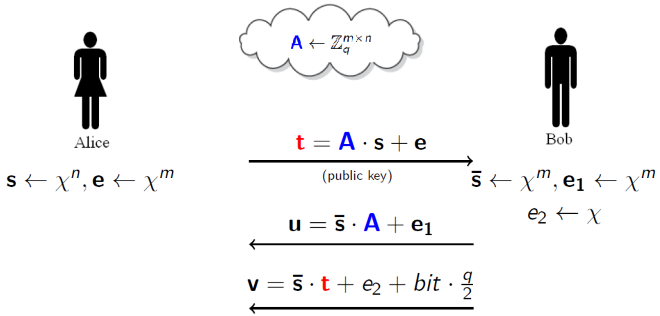
- Schema de mai sus criptează un bit iar decriptarea se face calculând $x = \mathbf{v} - \mathbf{u} \cdot \mathbf{s}$.

Sistem de criptare bazat pe LWE



- Schema de mai sus criptează un bit iar decriptarea se face calculând $x = \mathbf{v} - \mathbf{u} \cdot \mathbf{s}$.
- Rezultatul va fi 1 dacă x este mai aproape de $\frac{q}{2}$ decât de 0.

Sistem de criptare bazat pe LWE



- Schema de mai sus criptează un bit iar decriptarea se face calculând $x = \mathbf{v} - \mathbf{u} \cdot \mathbf{s}$.
- Rezultatul va fi 1 dacă x este mai aproape de $\frac{q}{2}$ decât de 0.
- Apropierea lui x de $\frac{q}{2}$ este verificată calculând valoarea absolută a lui $x - \frac{q}{2} \bmod q$

Sistem de criptare bazat pe LWE - securitate

- Decriptarea funcționeaza corect atâta timp cât $|\bar{\mathbf{s}} \cdot \mathbf{e} + e_2 - \mathbf{e_1} \cdot \mathbf{s}| < (q-1)/4$

Sistem de criptare bazat pe LWE - securitate

- Decriptarea funcționeaza corect atâta timp cât $|\bar{\mathbf{s}} \cdot \mathbf{e} + e_2 - \mathbf{e_1} \cdot \mathbf{s}| < (q-1)/4$
- Această condiție este îndeplinită dacă distribuția χ a valorilor $\mathbf{s}, \bar{\mathbf{s}}, \mathbf{e}, \mathbf{e_1}, e_2$ este aleasă corect și produce numere întregi suficient de mici.

Sistem de criptare bazat pe LWE - securitate

- Decriptarea funcționeaza corect atâta timp cât $|\bar{\mathbf{s}} \cdot \mathbf{e} + e_2 - \mathbf{e_1} \cdot \mathbf{s}| < (q-1)/4$
- Această condiție este îndeplinită dacă distribuția χ a valorilor $\mathbf{s}, \bar{\mathbf{s}}, \mathbf{e}, \mathbf{e_1}, e_2$ este aleasă corect și produce numere întregi suficient de mici.
- Sistemul de criptare este CPA-sigur (chiar și pentru adversari cuantici) dacă problema decizională LWE este dificilă.

Exerciții

Fie El Gamal cu $pk = (g, h = g^a)$ și $sk = (g, a)$ în $\mathbb{G}$.

- **Enc**: dată o cheie publică $(\mathbb{G}, q, g, h)$ și un mesaj $m \in \mathbb{G}$, alege $y \leftarrow^R \mathbb{Z}_q$ și întoarce $c = (c_1, c_2) = (g^y, m \cdot h^y)$;
- **Dec**: dată o cheie secretă $(\mathbb{G}, q, g, a)$ și un mesaj criptat $c = (c_1, c_2)$, întoarce $m = c_2 \cdot c_1^{-a}$.

Vrem să distribuim cheia secretă la două persoane așa încât numai cele două persoane împreună pot decripta. O modalitate simplă de a rezolva această problemă este să alegem două numere aleatoare $a_1, a_2 \in \mathbb{Z}_n$ așa încât $a_1 + a_2 = a$. O persoană primește a_1 iar cealaltă primește a_2. Pentru decriptarea (c_1, c_2), trimitem c_1 ambelor persoane.

Ce valori trebuie să calculeze cele două persoane și să ne trimită înapoi așa încât să putem decripta textul criptat trimis?

Exerciții

Fie El Gamal cu $pk = (g, h = g^a)$ și $sk = (g, a)$ în $\mathbb{G}$.

- **Enc**: dată o cheie publică $(\mathbb{G}, q, g, h)$ și un mesaj $m \in \mathbb{G}$, alege $y \leftarrow^R \mathbb{Z}_q$ și întoarce $c = (c_1, c_2) = (g^y, m \cdot h^y)$;
- **Dec**: dată o cheie secretă $(\mathbb{G}, q, g, a)$ și un mesaj criptat $c = (c_1, c_2)$, întoarce $m = c_2 \cdot c_1^{-a}$.

Vrem să distribuim cheia secretă la două persoane așa încât numai cele două persoane împreună pot decripta. O modalitate simplă de a rezolva această problemă este să alegem două numere aleatoare $a_1, a_2 \in \mathbb{Z}_n$ așa încât $a_1 + a_2 = a$. O persoană primește a_1 iar cealaltă primește a_2. Pentru decriptarea (c_1, c_2), trimitem c_1 ambelor persoane.

Ce valori trebuie să calculeze cele două persoane și să ne trimită înapoi așa încât să putem decripta textul criptat trimis?

Solution

Persoana 1 trimite $u_1 = c_1^{a_1}$ *iar persoana 2 trimite* $u_2 = c_1^{a_2}$*. Produsul* $u_1 \cdot u_2 = c_1^{a_1+a_2} = c_1^a$ *împreună cu* c_2 *poate fi folosit la decriptare.*

Se consideră $H : \{0,1\}^* \rightarrow \{0,1\}^n$ o funcție hash rezistentă la a doua preimagine și rezistentă la coliziuni. Se definește o funcție $H^* : \{0,1\}^* \rightarrow \{0,1\}^{n+1}$ astfel:

$$H'(x) = \begin{cases} x||1 & \text{dacă } x \in \{0,1\}^n \\ H(x)||0 & \text{altfel} \end{cases}$$

Argumentați că H' este rezistentă la coliziuni.

Se consideră $H : \{0,1\}^* \rightarrow \{0,1\}^n$ o funcție hash rezistentă la a doua preimagine și rezistentă la coliziuni. Se definește o funcție $H^* : \{0,1\}^* \rightarrow \{0,1\}^{n+1}$ astfel:

$$H'(x) = \begin{cases} x||1 & \text{dacă } x \in \{0,1\}^n \\ H(x)||0 & \text{altfel} \end{cases}$$

Argumentați că H' este rezistentă la coliziuni.

Solution

Fie $H'(x_1) = H'(x_2)$ cu $x_1 \neq x_2$. Dacă $H'(x_1) = x||1$ rezultă $x_1 = x_2$, contradicție. Dacă $H'(x_1) = H(x_1)||0 = H(x_2)||0$ atunci se determină o coliziune pentru H, contradicție.

Fie (Mac, Vrfy) un MAC sigur definit peste (K,M,T) unde $M = \{0,1\}^n$ și $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Argumentați răspunsul.

$$Mac'(k,m) = Mac(k,m)$$
$$Vrfy'(k,m,t) = \begin{cases} Vrfy(k,m,t), & \text{dacă } m \neq 0^n \\ 1, & \text{altfel} \end{cases}$$

Fie (Mac, Vrfy) un MAC sigur definit peste (K,M,T) unde $M = \{0,1\}^n$ și $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Argumentați răspunsul.

$$Mac'(k,m) = Mac(k,m)$$
$$Vrfy'(k,m,t) = \begin{cases} Vrfy(k,m,t), & \text{dacă } m \neq 0^n \\ 1, & \text{altfel} \end{cases}$$

Solution

MAC-ul nu este sigur pentru ca un adversar poate sa intoarca perechea validă $(0^n, 0^s)$.