Lattice-based cryptography: security foundations and constructions

Adeline Langlois

EPFL, Lausanne, Switzerland

Cryptography

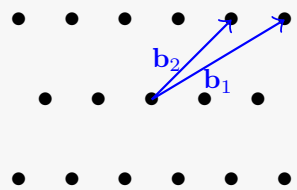
New challenges in cryptography

- Need of new functionalities,
- Quantum computers.

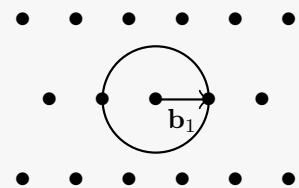
Lattice-based cryptography

- Is it a credible alternative to modern cryptography?
  - Functionality
  - Security
  - Efficiency
- Study of the new functionalities:
  - Fully homomorphic encryption,
  - Cryptographic multilinear maps.

Lattice

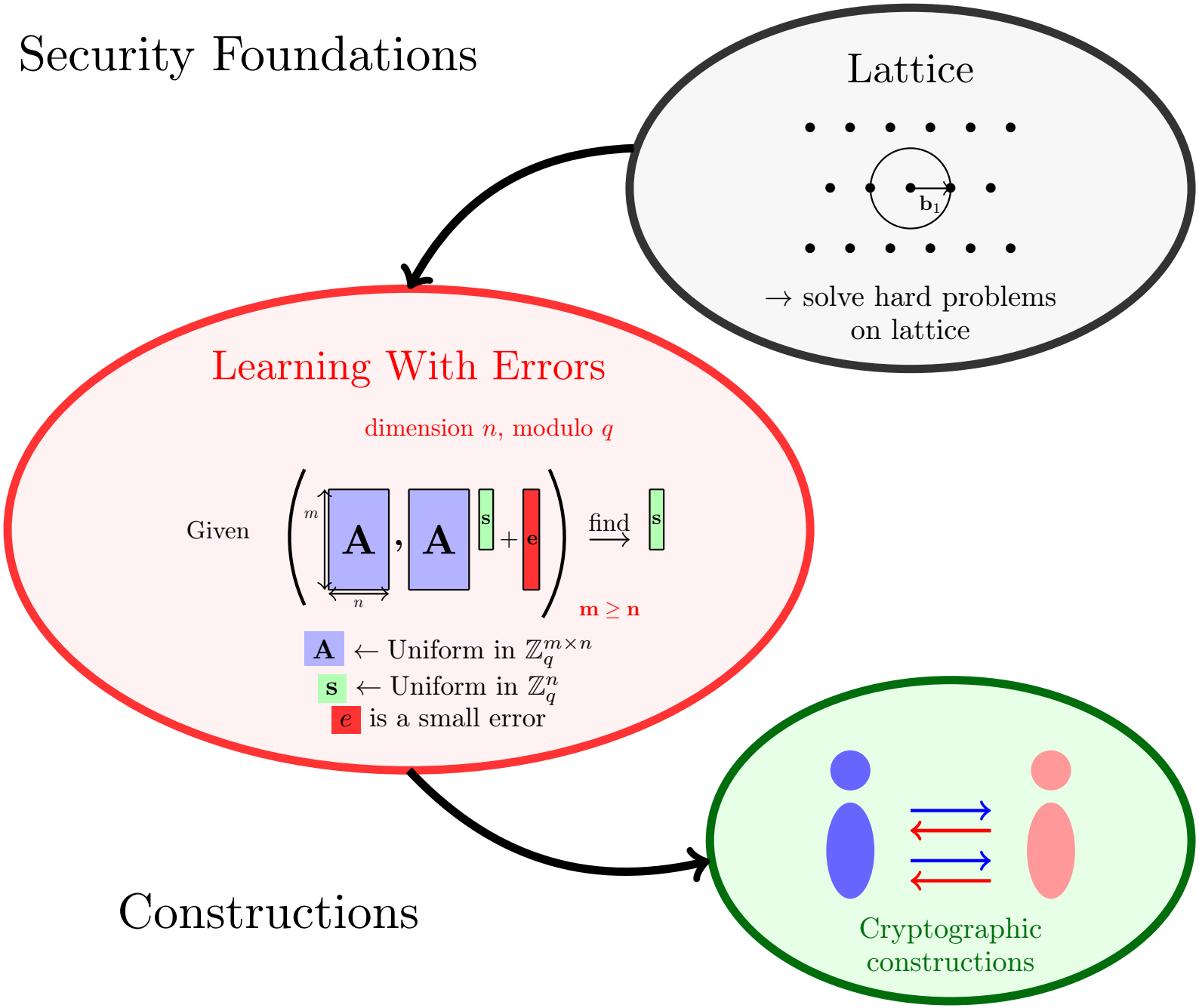


Lattice



Shortest Vector Problem

Security Foundations



Constructions

Lattice-based cryptography

Advantages

- (Asymptotically) efficient;
- Most security proofs **from the hardness of lattice problems**;
- Likely to resist attacks from quantum computers.

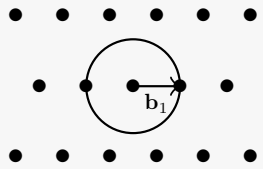
From basic to very advanced primitives

- Public key encryption and signature scheme (practical) ...
- New functionalities
  - Fully homomorphic encryption,
  - Cryptographic multilinear maps and applications.

My results

Classical hardness of LWE

Lattice



→ solve hard problem on lattice

Learning With Errors

dimension n, modulo q

Given $\left(\begin{array}{c|c|c} \mathbf{A} & \mathbf{A}\,\mathbf{s}+\mathbf{e} \end{array}\right)$ find $\mathbf{s}$

m rows, n columns

$\mathbf{m} \geq \mathbf{n}$

and/or SIS

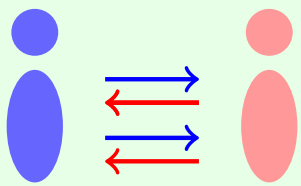
$\mathbf{A} \leftarrow$ Uniform in $\mathbb{Z}_q^{m \times n}$

$\mathbf{s} \leftarrow$ Uniform in $\mathbb{Z}_q^n$

e is a small error

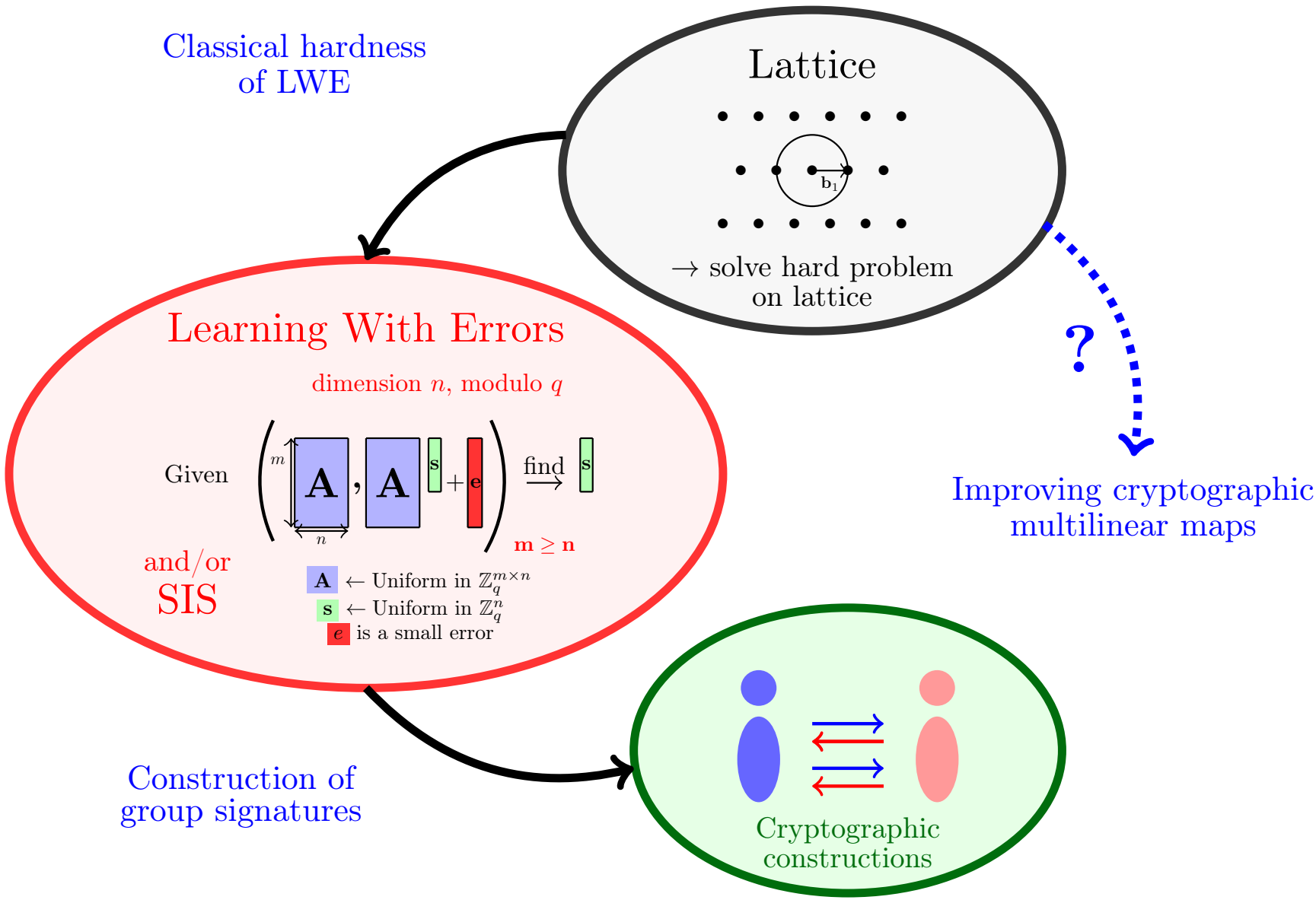
Improving cryptographic multilinear maps

Construction of group signatures



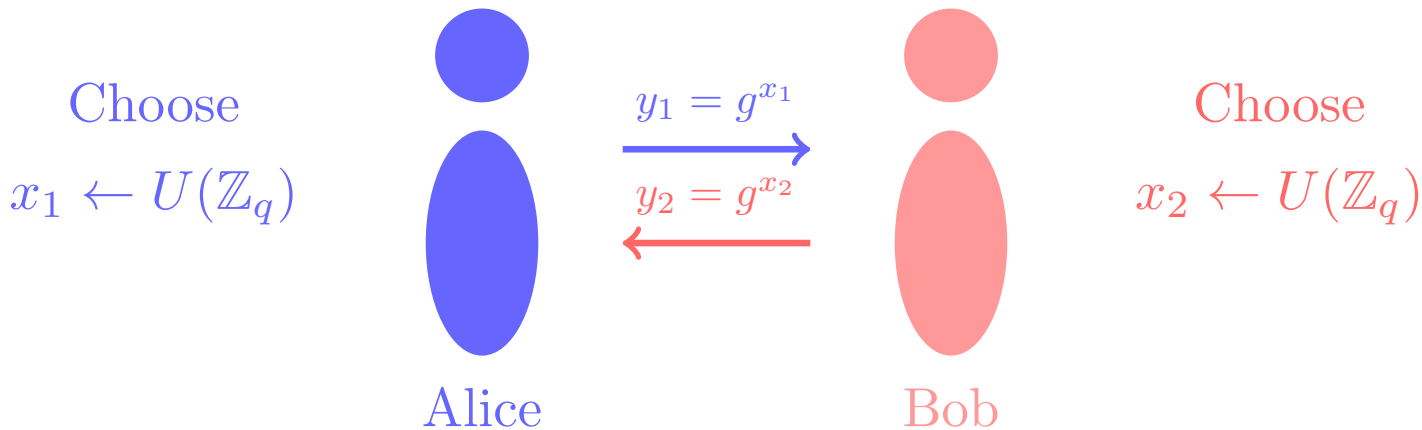
Cryptographic constructions

My results


Classical hardness
of LWE
Lattice
b_1
→ solve hard problem
on lattice
?
Improving cryptographic
multilinear maps
Learning With Errors
dimension n, modulo q
Given
m
n
A
A
s
e
find
s
$\mathbf{m \geq n}$
and/or
SIS
A ← Uniform in $\mathbb{Z}_q^{m \times n}$
s ← Uniform in $\mathbb{Z}_q^n$
e is a small error
Construction of
group signatures
Cryptographic
constructions

Diffie-Hellman Key Exchange (1976)

$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ with q prime, g public generator of $\mathbb{Z}_q^*$.

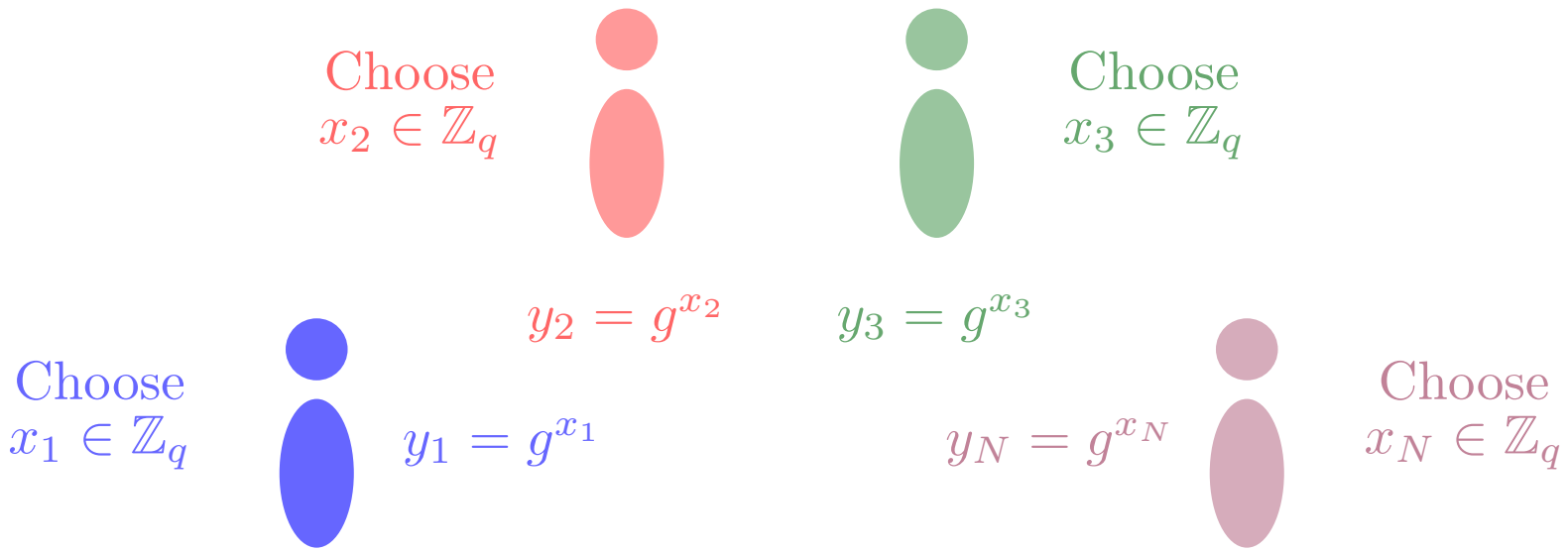


Agreed secret key: $K = g^{x_1 x_2} = y_1^{x_2} = y_2^{x_1}$

- Security: **Decisional Diffie-Hellman** problem.

Cryptographic Multilinear Maps – 21st Century variant

Group of $N > 2$ parties want to communicate privately via cloud.



Secret key (using e: "cryptographic multilinear map"):

$$K = e(g, \ldots, g)^{x_1 \cdots x_N} = e(y_2, y_3, \ldots, y_N)^{x_1} = e(y_1, y_3, \ldots, y_N)^{x_2}$$

Cryptographic Multilinear Maps

- 2013: [Garg, Gentry, Halevi 13]
  - First plausible realization for $N > 3$, via ideal lattices,
- 2014: GGHLite – More efficient variant of GGH,
  [Langlois, Stehlé, Steinfeld 14]
- Improving and implementing GGHLite – *work in progress.*
  [Albrecht, Cocis, Laguillaumie, Langlois]

N	n	$\log q$	Setup	Publish	KeyGen	|params|
7	65536	3605	2457s	12.58s	6.03s	112.7MB
26	262144	15410	29407s	465.36s	530.27s	1.4GB

- Open problems

  - Construction with a security proof?
    - Efficient for large N?

Cryptographic Multilinear Maps

- 2013: [Garg, Gentry, Halevi 13]
  - First plausible realization for $N > 3$, via ideal lattices,
- 2014: GGHLite – More efficient variant of GGH,

  [Langlois, Stehlé, Steinfeld 14]
- Improving and implementing GGHLite – *work in progress.*

  [Albrecht, Cocis, Laguillaumie, Langlois]

N	n	$\log q$	Setup	Publish	KeyGen	|params|
7	65536	3605	2457s	12.58s	6.03s	112.7MB
26	262144	15410	29407s	465.36s	530.27s	1.4GB

- Open problems

  - Construction with a security proof?
    - Efficient for large N?

Thank You