Anamorphism
Beyond One-To-One Messaging:
PKE with Anamorphic Broadcast Mode

Xuan Thanh Do Giuseppe Persiano Duong Hieu Phan Moti Yung

Institute of Cryptography Science and Technology,Vietnam.

Università di Salerno, Italy and Google LLC, USA.

Telecom Paris, Institut Polytechnique de Paris, France.

Google LLC and Columbia University, USA.

Anamorphism

Two-View Principle

Anamorphic Art: Two Views on the Same Object

In anamorphic art, an object can be seen from many viewpoints, but the “complete” image only appears from a specific angle.

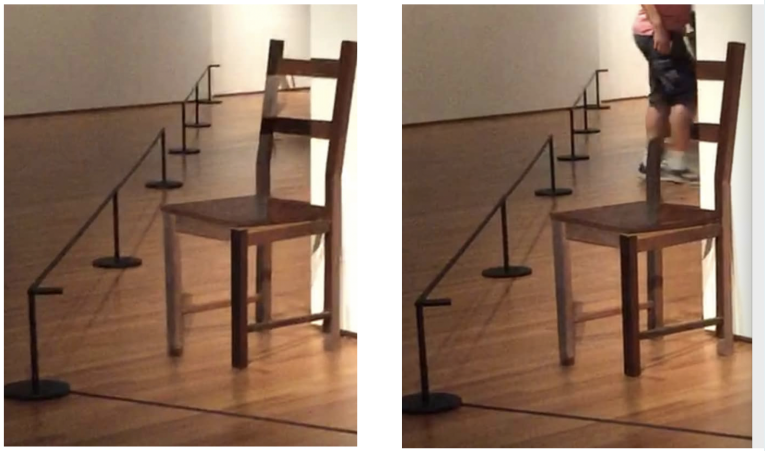
Two-View Principle

Anamorphic Art: Two Views on the Same Object

These images (*which I took at the National Gallery Singapore*) contain a proof of *anamorphism*: only from my specific position does the complete chair become visible.

Two-View Principle

Anamorphic Art: Two Views on the Same Object



Cryptography: Two Views on the "Same" Communication

- **Real view:** Actual interactions between insiders (holders of secret keys).
- **Simulated view:** Interactions are produced by a simulator.

Security: Real view $\approx$ *Simulated view* (e.g., ZKP, MPC)

Anamorphic Cryptography

[PPY22]

Anamorphic Ciphertext

$\xrightarrow{\textit{View with normal\_key}}$ a regular message

$\xrightarrow{\textit{View with double\_key}}$ *an anamorphic message*

Everything should look normal to a powerful adv. $\mathcal{D}$ (dictator):

Anamorphic Cryptography

[PPY22]

Anamorphic Ciphertext

$\xrightarrow{\textit{View with normal\_key}}$ a regular message

$\xrightarrow{\textit{View with double\_key}}$ *an anamorphic message*

Everything should look normal to a powerful adv. $\mathcal{D}$ (dictator):

- **Ciphertext rule:**

  Anamorphic ciphertexts $\overset{\mathcal{D}}{\approx}$ normal ciphertexts,

  for an allowed encryption, with a specific public key.
- **Key rule:** $\mathcal{D}$ can request the secret key corresponding to any public key (unlike in *steganography*).

Anamorphic Ciphertext

$\xrightarrow{\textit{View with normal\_key}}$ a regular message

$\xrightarrow{\textit{View with double\_key}}$ *an anamorphic message*

Everything should look normal to a powerful adv. $\mathcal{D}$ (dictator):

- **Ciphertext rule:**

  Anamorphic ciphertexts $\overset{\mathcal{D}}{\approx}$ normal ciphertexts,

  for an allowed encryption, with a specific public key.
- **Key rule:** $\mathcal{D}$ can request the secret key corresponding to any public key (unlike in *steganography*).
- **(New) Blocking rule:** *D* can block any party from receiving communications (the fraction of blocked parties

Crypto War: On the User's Side

The dictator enacts a law mandating weakened encryption or a built-in backdoor.

$\rightarrow$ A huge risk for **everyone**, including the dictator (e.g., Clipper chip, Dual_EC_DRBG).

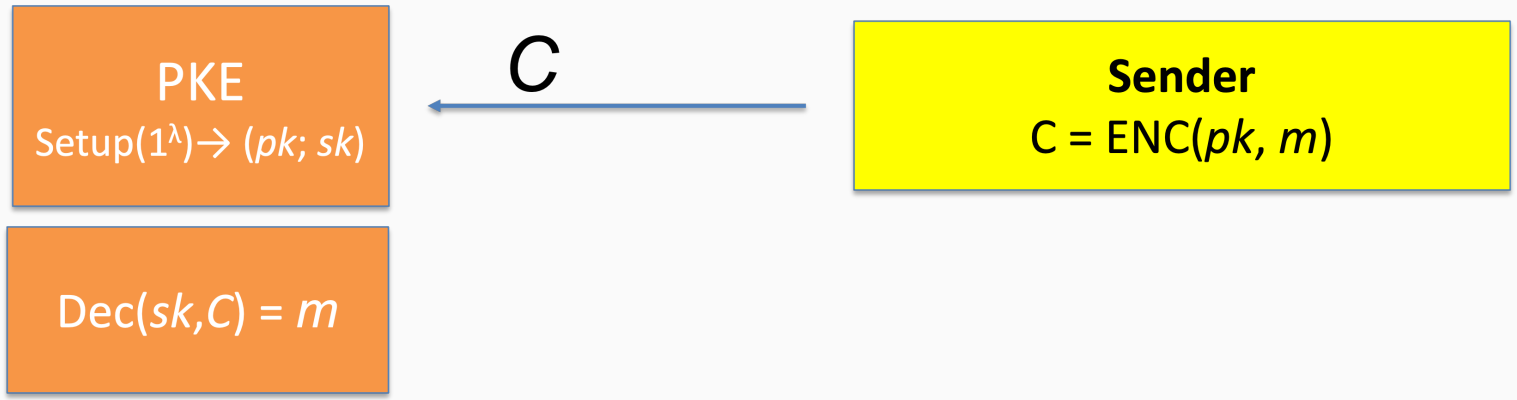
Solution: Public debate, petitions, or technical demonstrations to oppose the approval of such laws.

The dictator permits standard encryption but remotely and massively controls all users:

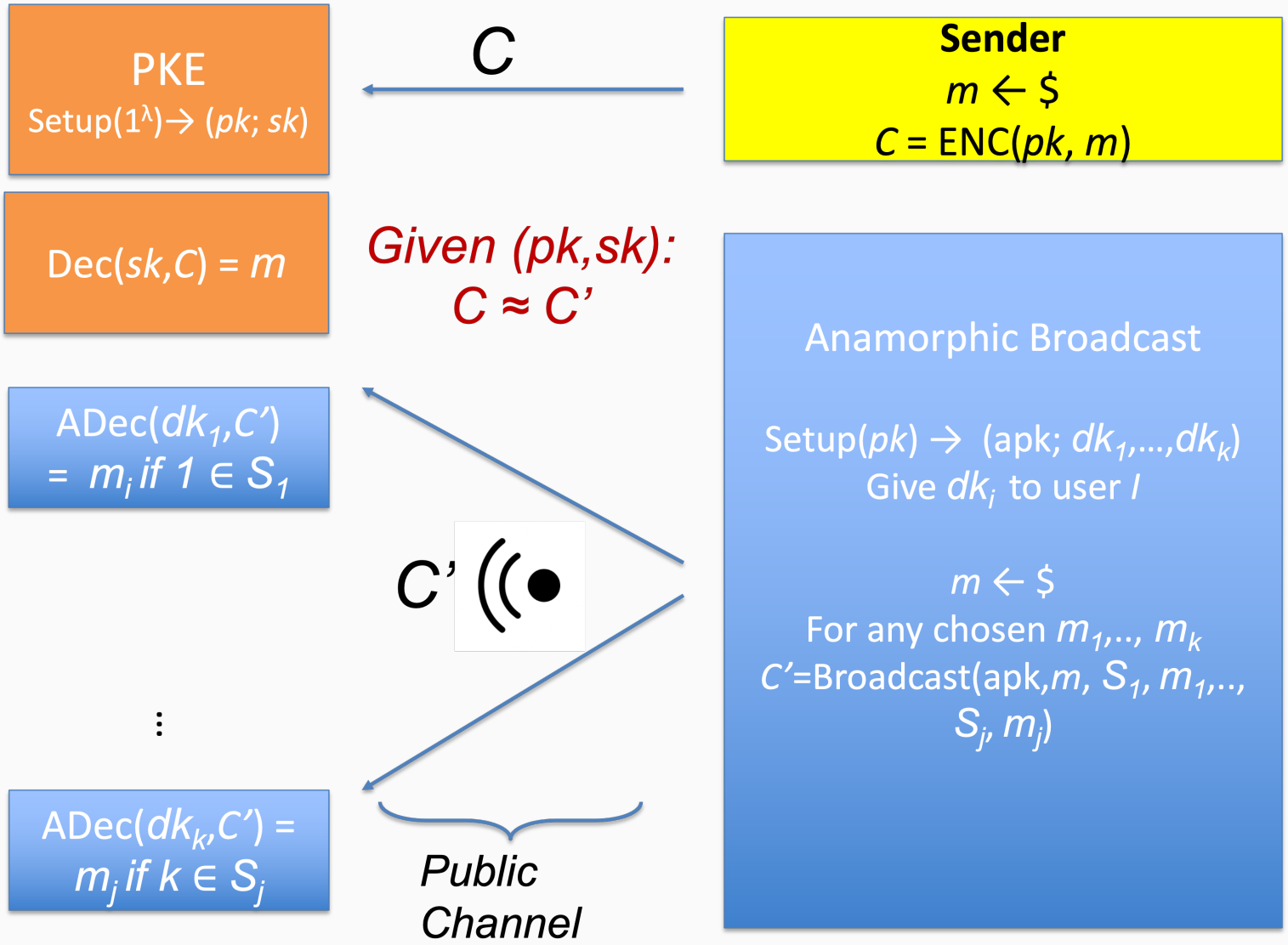
- Require receivers to surrender their **secret keys** so all messages can be decrypted.
- **Block** any suspected users.

Our proposed **anamorphic model** provides a way to preserve users' privacy in this scenario.

PKE with Anamorphic Broadcast Mode



PKE with Anamorphic Broadcast Mode



Our Construction

Anonymity to Anamorphism: from Anonymous Multi-channel Broadcast (AnonMCBE)

Generic Approach

PKE + Associated Anonymous Multi-channel Broadcast such that the ciphertexts are indistinguishable.
Then we can obtain PKE with Anamorphic Broadcast Mode.

How does it work?

- The sender sets up the AnonMCBE.
- Instead of sending a PKE ciphertext, they send a AnonMCBE's ciphertext.
- Anonymity + PKE ciphertexts $\approx$ AnonMCBE ciphertexts
  $\rightarrow$ Everything appears normal to the dictator.
- Double keys are decryption keys of AnonMCBE.
- Each anamorphic user decrypts to a message depending on the channel they belong to.

Anamorphic Broadcast: Instantiation

Generic Approach

PKE + Associated Anonymous Multi-channel Broadcast
such that: the ciphertexts are indistinguishable
then we can get PKE with Anamorphic Broadcast Mdoe.

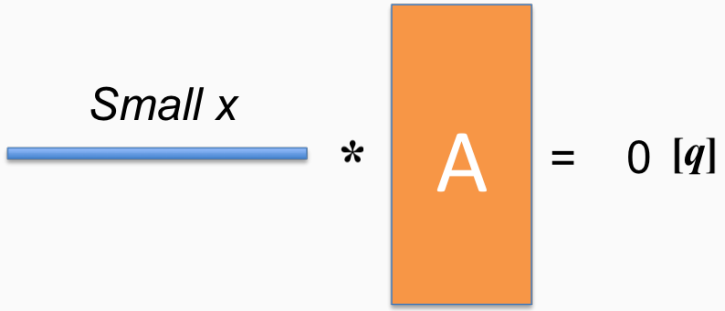
Concrete Construction based on previous works:

- Multi-channel Broadcast [PPT12]: not anonymous.
- Multi-receiver Encryption [LPSS14]: 1 channel, ciphertext is of the same form as in PKE.
- Anonymous Broadcast [DPY20]: 1 channel, ciphertext is of the same form as in PKE.

Our Scheme: Anonymous Multi-channel Broadcast: many channels, ciphertext is of the same form as in PKE.

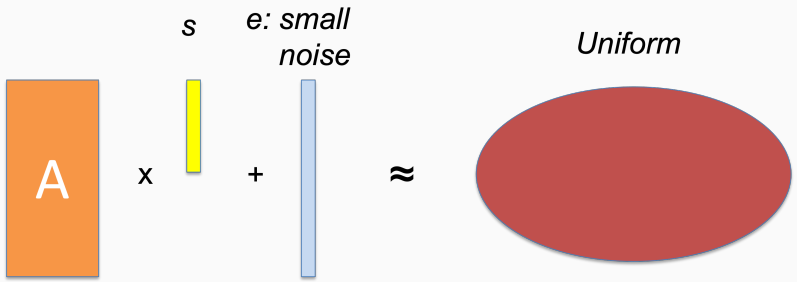
Short Integer Solution [Ajtai96] and Learning With Errors [Regev05] problems

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$



SIS

Find small $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$ s.t. $\mathbf{x}^t A = \mathbf{0}\ [q]$



Key Idea for 1-bit PKE:
w.o secret key x : U(Im(A)) + noise ≈ *Uniform*
with secret key x : x * U(Im(A)) + noise → *small*

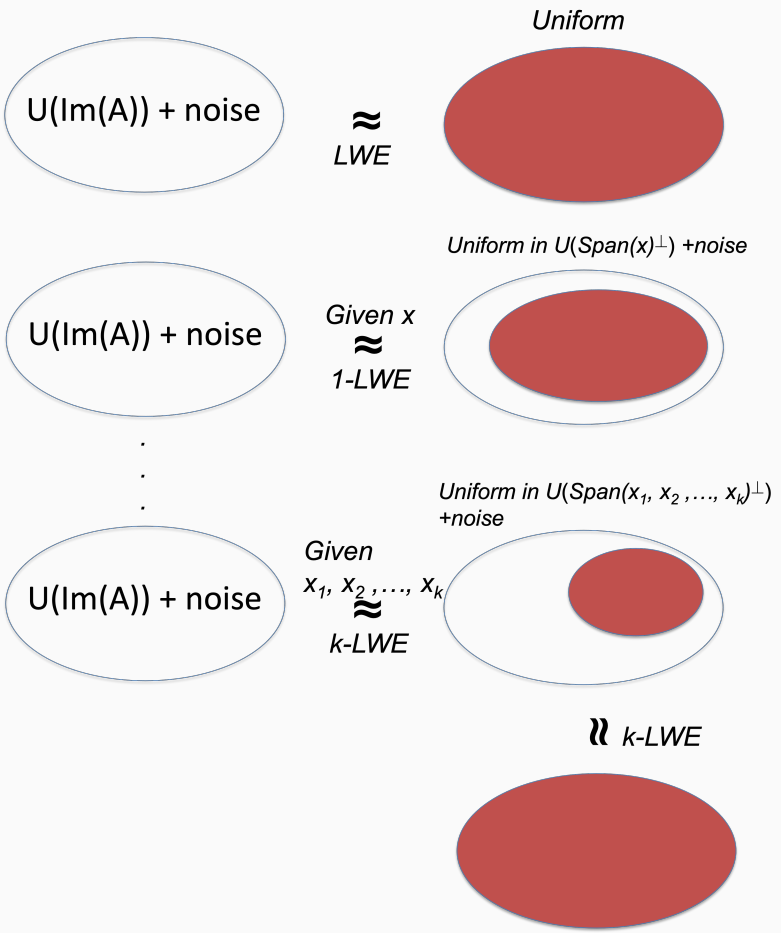
(Here, A *denotes* $\frac{\text{A}}{\text{u}}$ *in Dual Regev LWE Encryption*)

LWE

Dist. $A\mathbf{s} + \mathbf{e}\ [q]$ and $U(\mathbb{Z}_q^m)$, for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, noise $\mathbf{e} \in \mathbb{Z}^m$

k-LWE and Anonymous Broadcast

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$
- Given k small hints $(\mathbf{x}_i)_{i \leq k}$ s.t. $\mathbf{x}_i^t A = \mathbf{0}\ [q]$ (from [GPV08])



k-SIS [BF11]

Find small $\mathbf{x} \in \mathbb{Z}^m$ s.t.

- $\mathbf{x}^t A = \mathbf{0}\ [q]$
- $\mathbf{x} \notin \mathrm{Span}_{i \leq k}(\mathbf{x}_i)$

k-LWE [LPSS14]

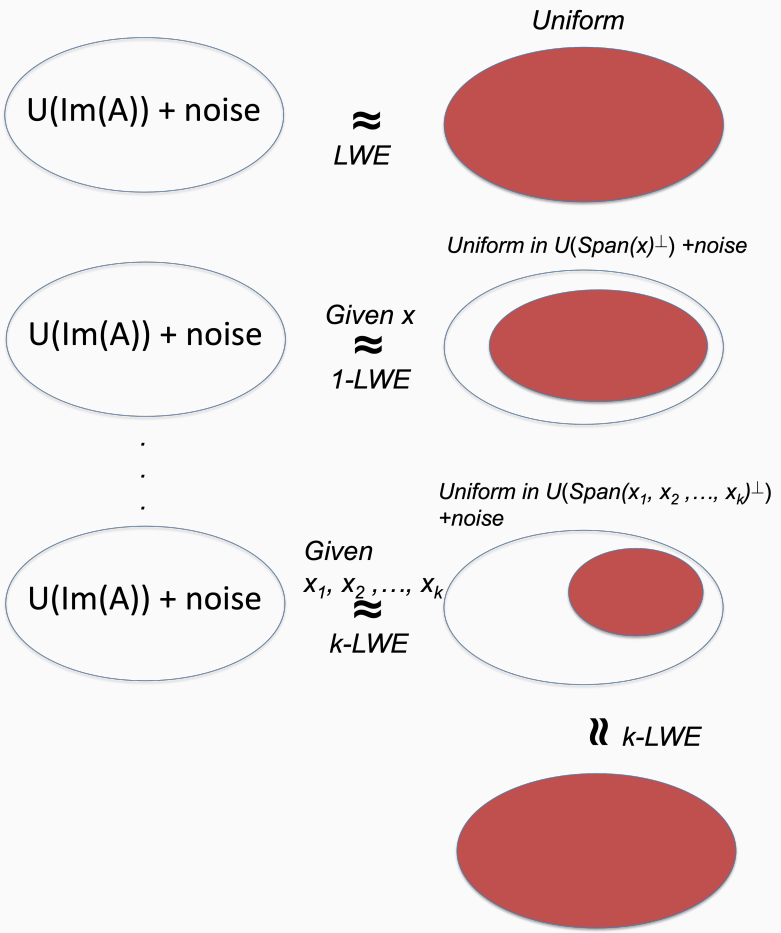
Distinguish $A\mathbf{s} + \mathbf{e}$ and $U(\mathrm{Span}_{i \leq k}(\mathbf{x}_i)^\perp) + \mathbf{e}'$ for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$ and small noises $\mathbf{e}, \mathbf{e}' \in \mathbb{Z}^m$

Anon-Broadcast [DPY20]

Using $U(\mathrm{Span}_{i \leq k}(\mathbf{x}_i)^\perp) + \mathbf{e}'$

k-LWE and Anonymous Broadcast

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$
- Given k small hints $(\mathbf{x}_i)_{i \leq k}$ s.t. $\mathbf{x}_i^t A = \mathbf{0}\ [q]$ (from [GPV08])



k-SIS [BF11]

Find small $\mathbf{x} \in \mathbb{Z}^m$ s.t.

- $\mathbf{x}^t A = \mathbf{0}\ [q]$
- $\mathbf{x} \notin \mathrm{Span}_{i \leq k}(\mathbf{x}_i)$

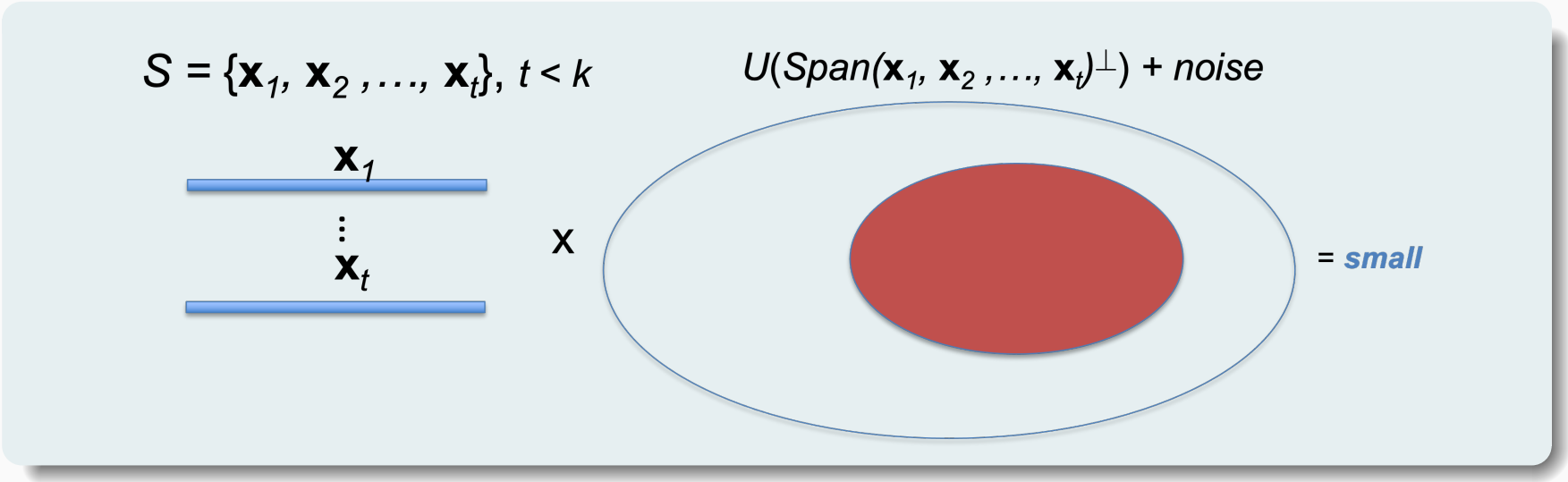
k-LWE [LPSS14]

Distinguish $A\mathbf{s} + \mathbf{e}$ and $U(\mathrm{Span}_{i \leq k}(\mathbf{x}_i)^\perp) + \mathbf{e}'$ for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$ and small noises $\mathbf{e}, \mathbf{e}' \in \mathbb{Z}^m$

Anon-Broadcast [DPY20]

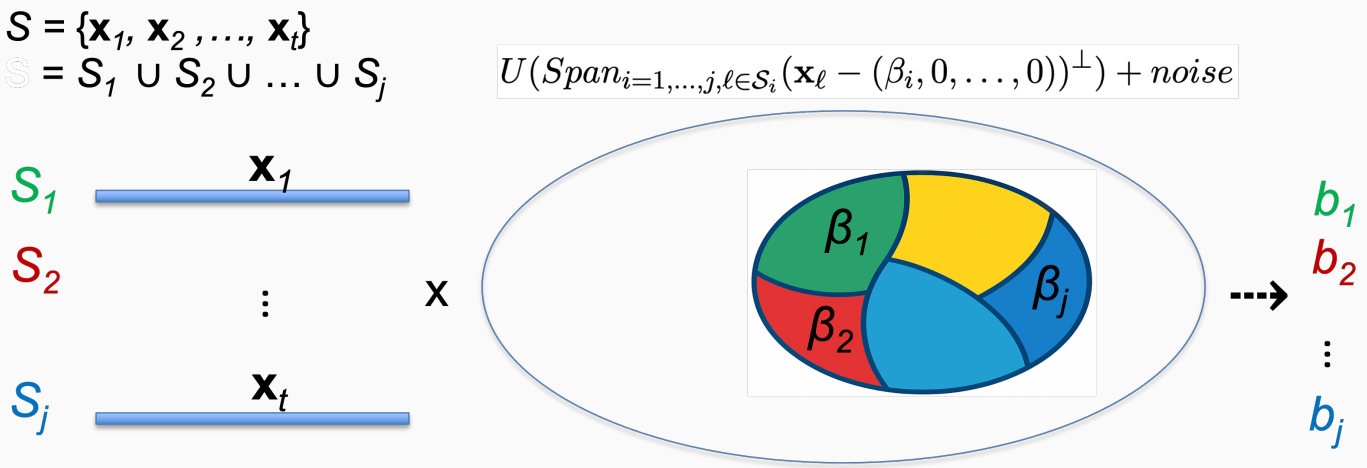
Using $U(\mathrm{Span}_{i \leq k}(\mathbf{x}_i)^\perp) + \mathbf{e}'$

Anonymous Broadcast Encryption from k-LWE in a Bounded Universe of k Users



- Twist on [LPSS14]: Using $U(\mathrm{span}_{i \le t}(\mathbf{x}_i)^{\perp}) + \mathbf{e}$ for broadcasting (instead of tracing).
- Any user $\mathbf{x}_i$ can decrypt (while all others receive a random bit), and the ciphertext remains indistinguishable from standard PKE ciphertexts, under the k-LWE assumption.

Anonymous Multi-channel Broadcast Encryption



- 1-channel: Using $\mathbf{y} \hookleftarrow U(\mathrm{Span}_{i\leq t}(\mathbf{x}_i - (\beta, 0, \ldots, 0))^\perp) + \mathbf{e}$ to broadcast, then the decrypted result is modified, depending on βy_1 (all users in S still get the same result).
- **Multi-channel**: Partition the set into $S_1, \ldots, S_j$, where each set S_i is associated with $\beta_i \rightarrow$ anyone in the same subset decrypts to the same bit (depending on $\beta_i y_1$).

Discussion and Open Questions

Anamorphic Crypto: Recent Active Directions

- Sender Anamorphism: The dictator can ask the sender to encrypt a specific message and provide proof of doing so (by giving him the randomness).
- Robustness; Anamorphic Extensions;
- Anamorphic-Resistance Encryption (ARE),
- Anamorphism in other primitives such as Signature, FHE.
- Public-key Anamorphism: No shared double keys.
- Generic constructions for any scheme? ($\rightarrow$ next talk.)

Open questions

- Extend the one-to-many channel model along the above directions, in particular public-key anamorphism.
- Anamorphic broadcast mode for more schemes?
  $\rightarrow$ Bounded-Collusion Anonymous Broadcast Encryption.