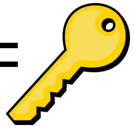
Bounded-Collusion IBE from Semantically-Secure PKE:
Generic Constructions with Short Ciphertexts

Stefano Tessaro (UC Santa Barbara)
David A. Wilson (MIT)

Bounded-Collusion IBE from Semantically-Secure PKE:
Generic Constructions with Short Ciphertexts

PKE = (Gen, Enc, Dec)

pk= 

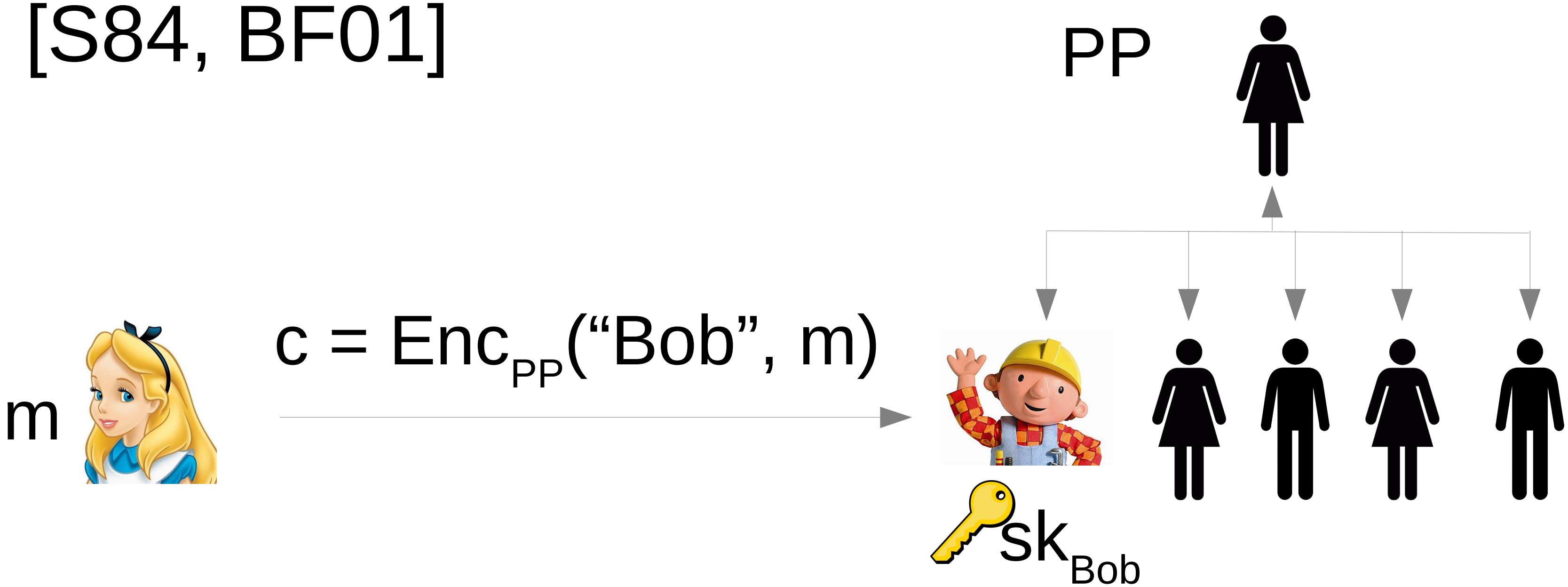
m  $c = \mathrm{Enc}_{pk}(m)$ →  sk= 

$m = \mathrm{Dec}_{sk}(c)$

Semantic security [GM84]: $\mathrm{Enc}_{pk}(m) \approx \mathrm{Enc}_{pk}(0)$

Bounded-Collusion IBE from Semantically-Secure PKE:
Generic Constructions with Short Ciphertexts

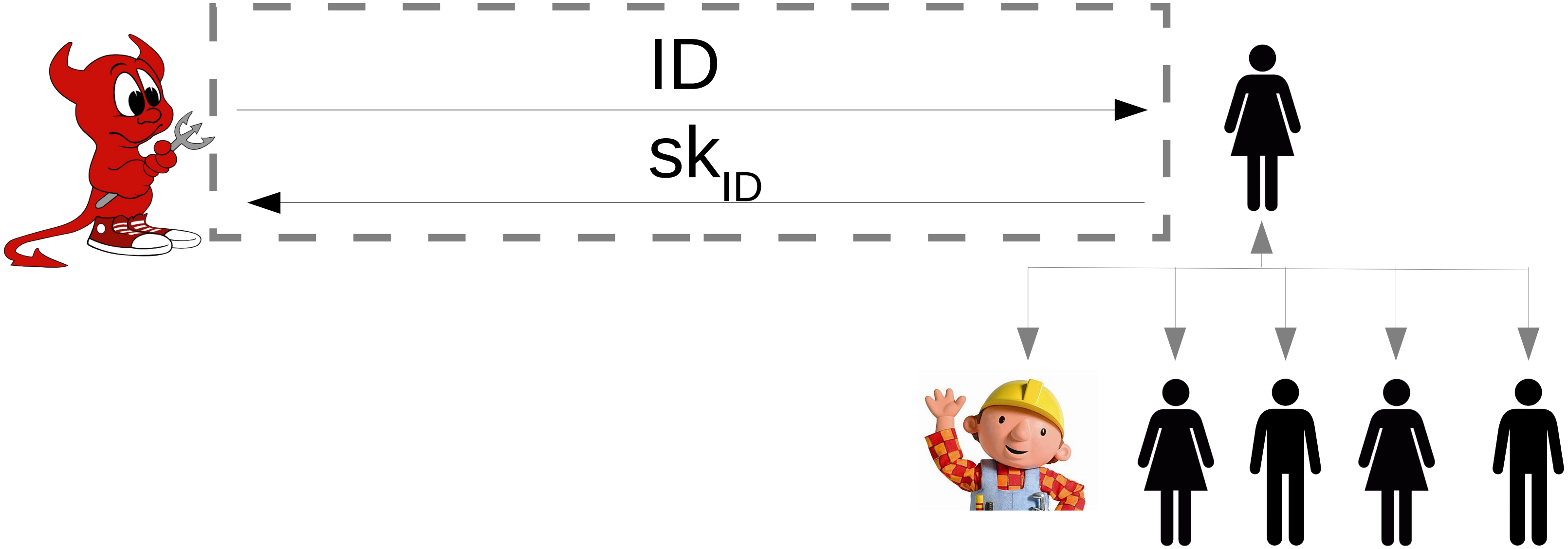
- Users have identities; encryption only requires global public parameters and recipient's identity
- IBE = (IBEGen, IBEExtract, IBEEnc, IBEDec)
- [S84, BF01]



Bounded-Collusion IBE from Semantically-Secure PKE:

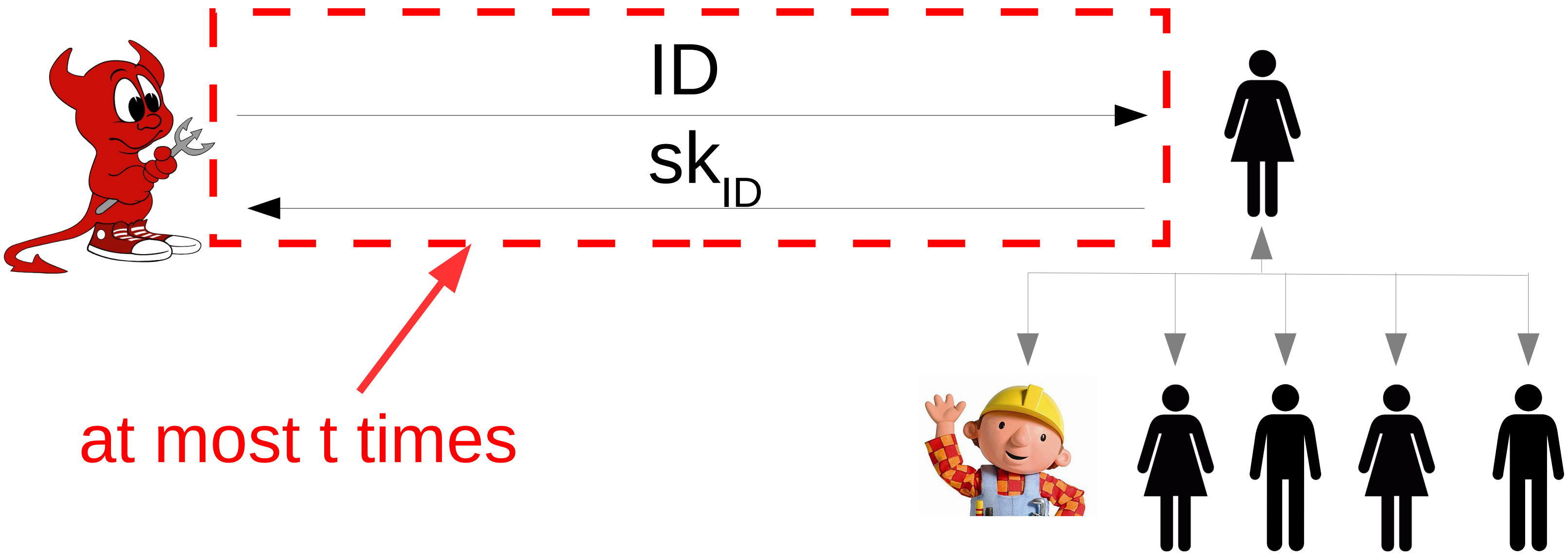
Generic Constructions with Short Ciphertexts

- Adversary is allowed to obtain keys for arbitrary identities
- Semantic security: Adversary must distinguish messages for an unqueried identity
- Selective security: Adversary declares target ID at start



Bounded-Collusion IBE from Semantically-Secure PKE:
Generic Constructions with Short Ciphertexts

- Same definition for full and selective security, except we place an a priori bound t on the number of ID queries adversary can make
- |PP| may depend on t



Bounded-Collusion IBE from Semantically-Secure PKE:

Generic Constructions with Short Ciphertexts

	Assumptions	Ciphertext Size	PP Size
[GLW12]	PKE w/linear hash proof; key homomorphism	Same as underlying PKE	Θ(t lg |ID|) PKE PKs
[DKXY02]	Semantic-secure PKE	Θ(t lg |ID|) PKE ciphertexts	$\Theta(t^2$ lg |ID|) PKE PKs
This work	Semantic-secure PKE; key homomorphism; weak multi-key malleability	**Same as underlying PKE**	$\Theta(t^2$ lg |ID|) PKE PKs
This work	Semantic-secure PKE; multi-key malleability	**Same as underlying PKE**	$\Theta(t^2$ lg |ID|) PKE PKs
[DKXY02]	DDH	3 group elements	Θ(t lg |ID|) elts
[GLW12]	DDH	3 group elements	Θ(t lg |ID|) elts
This work	DDH	**2 group elements**	$\Theta(t^2$ lg |ID|) elts
[GLW12]	QR	2 RSA group elements	Θ(t lg |ID|) elts
This work	LWE	**Same as [GPV08]**	$\Theta(t^2$ lg |ID|) PKs
This work	NTRU	**Same as [HPS98]**	$\Theta(t^2$ lg |ID|) PKs

Bounded-Collusion IBE from Semantically-Secure PKE:

Generic Constructions with ~~Short Ciphertexts~~

	Assumptions	**Ciphertext Size**	**PP Size**
[GLW12]	PKE w/linear hash proof; key homomorphism	Same as underlying PKE	Θ(t lg |ID|) PKE PKs
[DKXY02]	Semantic-secure PKE	Θ(t lg |ID|) PKE ciphertexts	Θ(t^2 lg |ID|) PKE PKs
This work	Semantic-secure PKE; key homomorphism; weak multi-key malleability	**Same as underlying PKE**	Θ(t^2 lg |ID|) PKE PKs
This work	Semantic-secure PKE; multi-key malleability	**Same as underlying PKE**	Θ(t^2 lg |ID|) PKE PKs
[DKXY02]	DDH	3 group elements	Θ(t lg |ID|) elts
[GLW12]	DDH	3 group elements	Θ(t lg |ID|) elts
This work	DDH	**2 group elements**	Θ(t^2 lg |ID|) elts
[GLW12]	QR	2 RSA group elements	Θ(t lg |ID|) elts
This work	LWE	**Same as [GPV08]**	Θ(t^2 lg |ID|) PKs
This work	NTRU	**Same as [HPS98]**	Θ(t^2 lg |ID|) PKs

Bounded-Collusion IBE from Semantically-Secure PKE:

~ Generic Constructions with Short Ciphertexts

	Assumptions	**Ciphertext Size**	**PP Size**
[GLW12]	PKE w/linear hash proof; key homomorphism	Same as underlying PKE	Θ(t lg |ID|) PKE PKs
[DKXY02]	Semantic-secure PKE	Θ(t lg |ID|) PKE ciphertexts	$\Theta(t^2$ lg |ID|) PKE PKs
This work	Semantic-secure PKE; key homomorphism; weak multi-key malleability	**Same as underlying PKE**	$\Theta(t^2$ lg |ID|) PKE PKs
This work	Semantic-secure PKE; multi-key malleability	**Same as underlying PKE**	$\Theta(t^2$ lg |ID|) PKE PKs
[DKXY02]	DDH	3 group elements	Θ(t lg |ID|) elts
[GLW12]	DDH	3 group elements	Θ(t lg |ID|) elts
This work	DDH	**2 group elements**	$\Theta(t^2$ lg |ID|) elts
[GLW12]	QR	2 RSA group elements	Θ(t lg |ID|) elts
This work	LWE	**Same as [GPV08]**	$\Theta(t^2$ lg |ID|) PKs
This work	NTRU	**Same as [HPS98]**	$\Theta(t^2$ lg |ID|) PKs

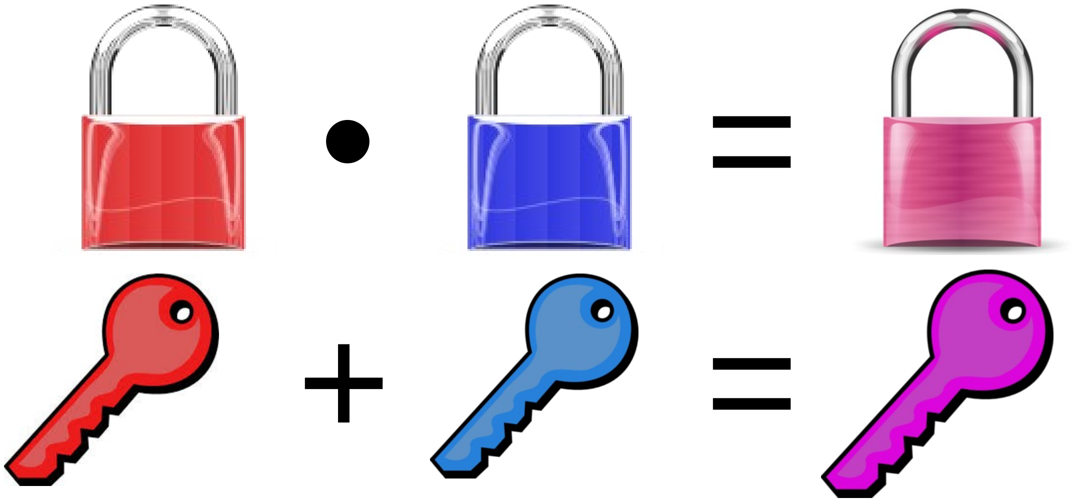
Bounded-Collusion IBE from Semantically-Secure PKE:

Generic Constructions with Short Ciphertexts

	Assumptions	Ciphertext Size	PP Size
[GLW12]	PKE w/linear hash proof; key homomorphism	Same as underlying PKE	Θ(t lg |ID|) PKE PKs
[DKXY02]	Semantic-secure PKE	Θ(t lg |ID|) PKE ciphertexts	$\Theta(t^2$ lg |ID|) PKE PKs
This work	Semantic-secure PKE; key homomorphism; weak multi-key malleability	**Same as underlying PKE**	$\Theta(t^2$ lg |ID|) PKE PKs
This work	Semantic-secure PKE; multi-key malleability	**Same as underlying PKE**	$\Theta(t^2$ lg |ID|) PKE PKs
[DKXY02]	DDH	3 group elements	Θ(t lg |ID|) elts
[GLW12]	DDH	3 group elements	Θ(t lg |ID|) elts
This work	DDH	**2 group elements**	$\Theta(t^2$ lg |ID|) elts
[GLW12]	QR	2 RSA group elements	Θ(t lg |ID|) elts
This work	LWE	**Same as [GPV08]**	$\Theta(t^2$ lg |ID|) PKs
This work	NTRU	**Same as [HPS98]**	$\Theta(t^2$ lg |ID|) PKs

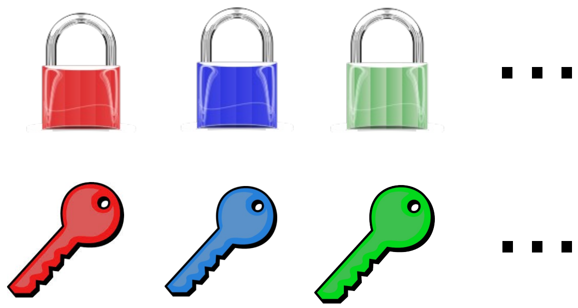
Key Homomorphism

- A public-key encryption scheme has a secret-key to public-key homomorphism μ if:
  - secret keys ∈ group G (group operation +)
  - public keys ∈ group H (group operation •)
  - (pk, sk) ← Gen implies pk = μ(sk)
  - ∀ sk, sk' ∈ G, μ(sk+sk') = μ(sk) • μ(sk')



GLW Construction

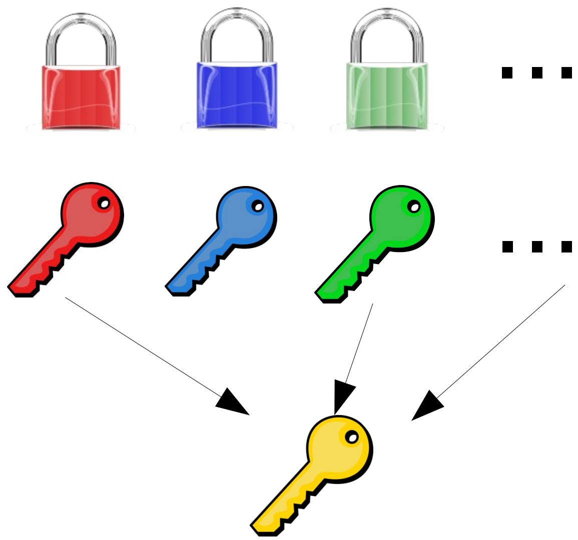
- Identity map φ: ID $\rightarrow \{0,1\}^n$ (view as subset)
- IBEGen: Run Gen^n
  - PP = $(pk_1,...pk_n)$
  - msk = $(sk_1,...sk_n)$



- IBEExtract:
  - $sk_{ID} = \sum_{i\in \varphi(ID)} sk_i$
- IBEEnc:
  - $pk_{ID} = \prod_{i\in \varphi(ID)} pk_i$
  - $c = Enc(pk_{ID}, m)$

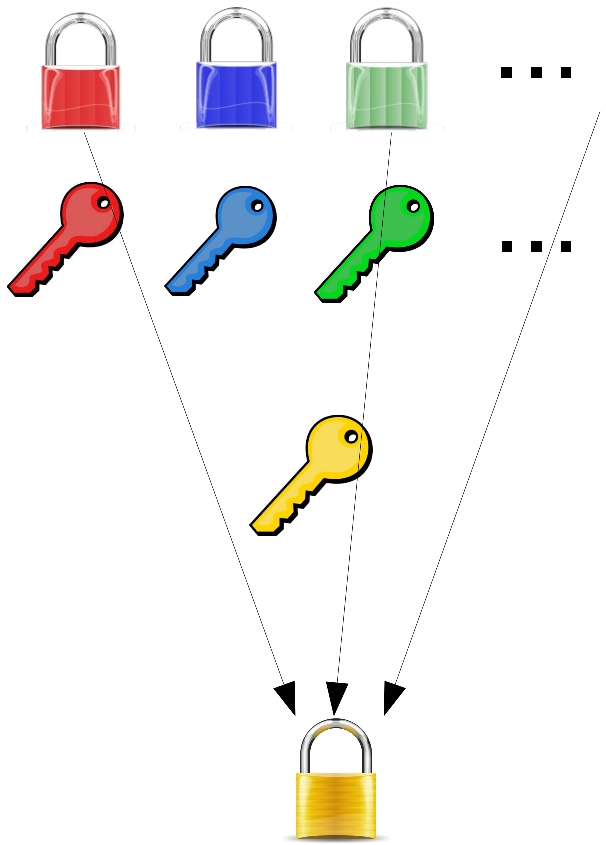
GLW Construction

- Identity map φ: ID → $\{0,1\}^n$ (view as subset)
- IBEGen: Run Gen^n
  - $PP = (pk_1,\ldots pk_n)$
  - $msk = (sk_1,\ldots sk_n)$
- IBEExtract:
  - $sk_{ID} = \sum_{i\in \varphi(ID)} sk_i$
- IBEEnc:
  - $pk_{ID} = \prod_{i\in \varphi(ID)} pk_i$
  - $c = Enc(pk_{ID}, m)$



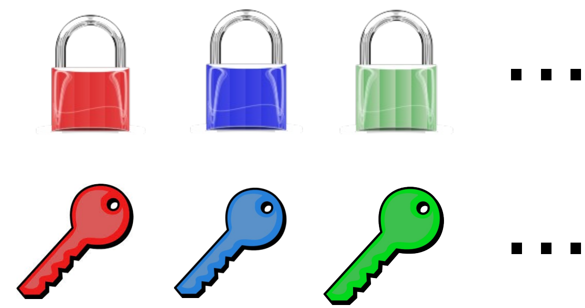
GLW Construction

- Identity map φ: ID → $\{0,1\}^n$ (view as subset)
- IBEGen: Run Gen^n
  - PP = $(pk_1,\ldots pk_n)$
  - msk = $(sk_1,\ldots sk_n)$
- IBEExtract:
  - $sk_{ID} = \sum_{i\in\varphi(ID)} sk_i$
- IBEEnc:
  - $pk_{ID} = \prod_{i\in\varphi(ID)} pk_i$
  - $c = \text{Enc}(pk_{ID}, m)$



GLW Construction

- Identity map φ: ID → $\{0,1\}^n$ (view as subset)
- IBEGen: Run Gen^n
  - PP = $(pk_1,\ldots pk_n)$
  - msk = $(sk_1,\ldots sk_n)$



- IBEExtract:
  - $sk_{ID} = \sum_{i\in\varphi(ID)} sk_i$

- IBEEnc:
  - $pk_{ID} = \prod_{i\in\varphi(ID)} pk_i$

  - $c = Enc(pk_{ID}, m)$

Cover-Free Maps

- What to use as φ?
- t-cover-free map: no group of t subsets completely "covers" another

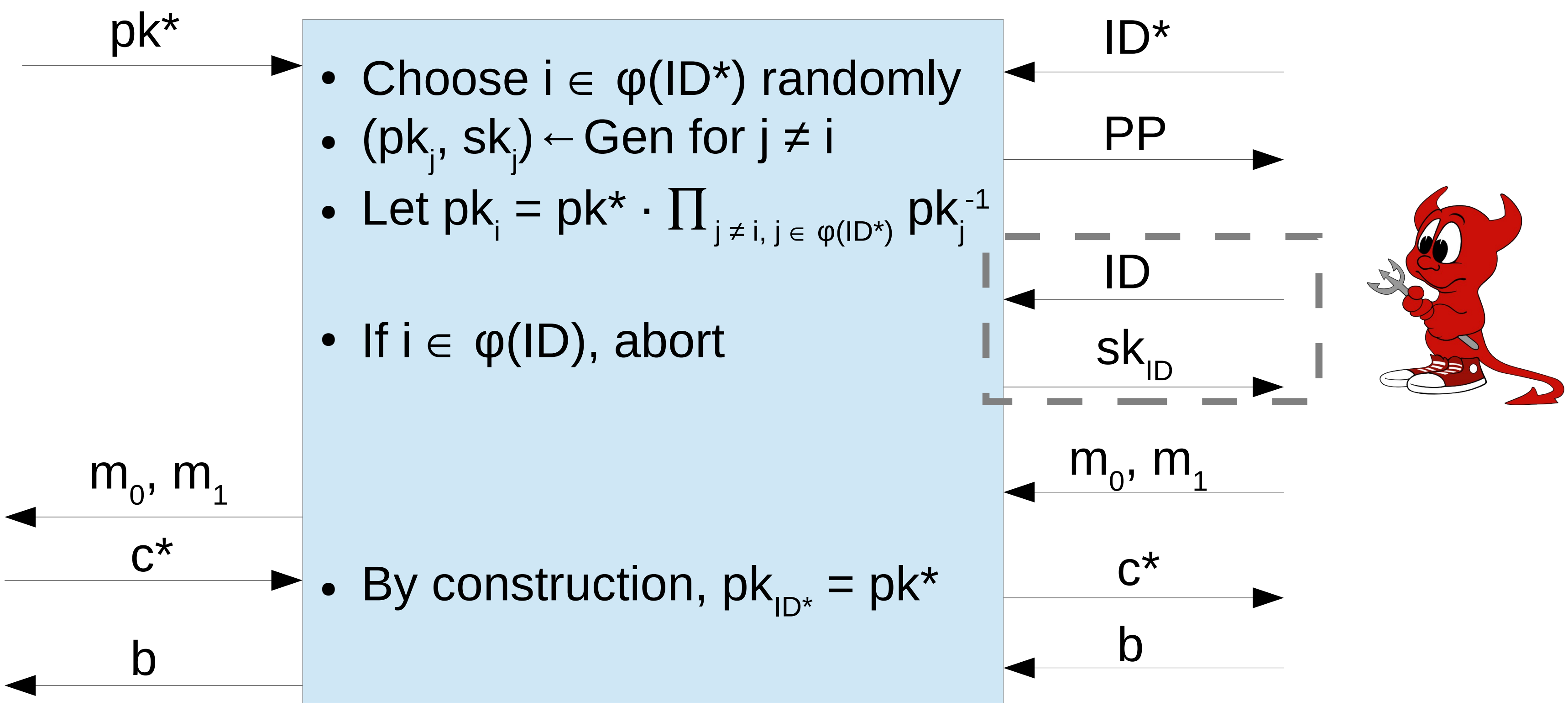
$$\forall ID_0, ID_1, \ldots ID_t,\ \ \varphi(ID_0) \setminus \bigcup_{i=1\ldots t} \varphi(ID_i) \neq \emptyset$$

(Note: We can make t-cover-free maps with $n=\Theta(t^2)$ that support exponentially many IDs in total. [CHH+07])

Selective Security of GLW

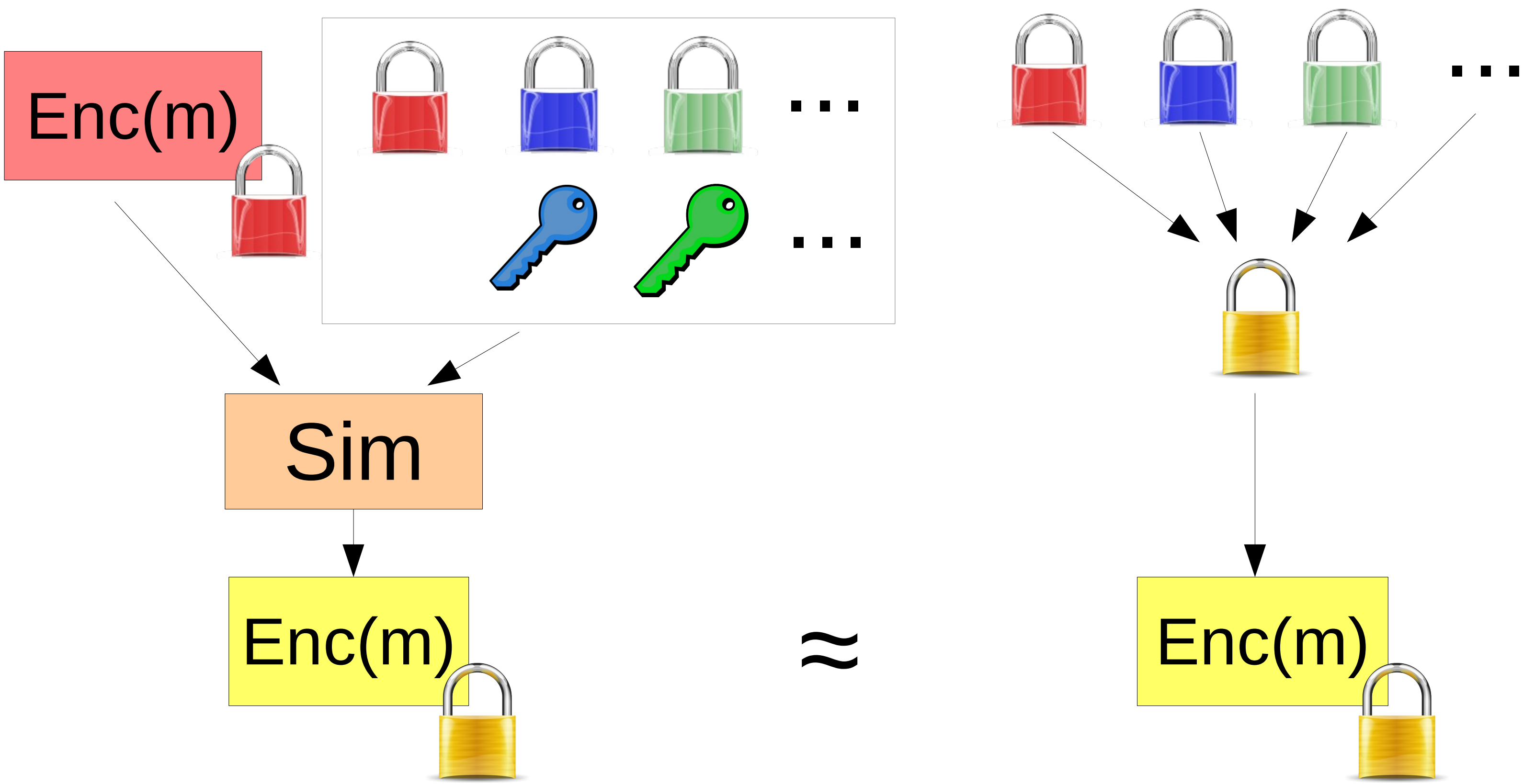
Thm. If PKE is semantically secure and φ is (t+1)-cover-free, then the GLW construction is a selectively-secure t-BC-IBE.

- Proof: guess the “uncovered” key in φ(ID*)



Weak Multi-Key Malleability

- PKE is weakly n-key malleable if ∃ PPT Sim that can convert a ciphertext of an unknown message to a ciphertext under the product of n keys, one of which is the original

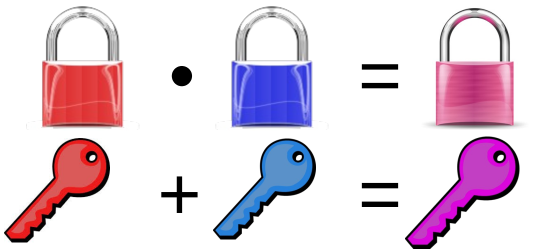


Full Security of GLW

Thm. If PKE is semantically secure and weakly n-key malleable, and φ is (t+1)-cover-free, then the GLW construction is a (fully) semantically-secure t-BC-IBE.

Example

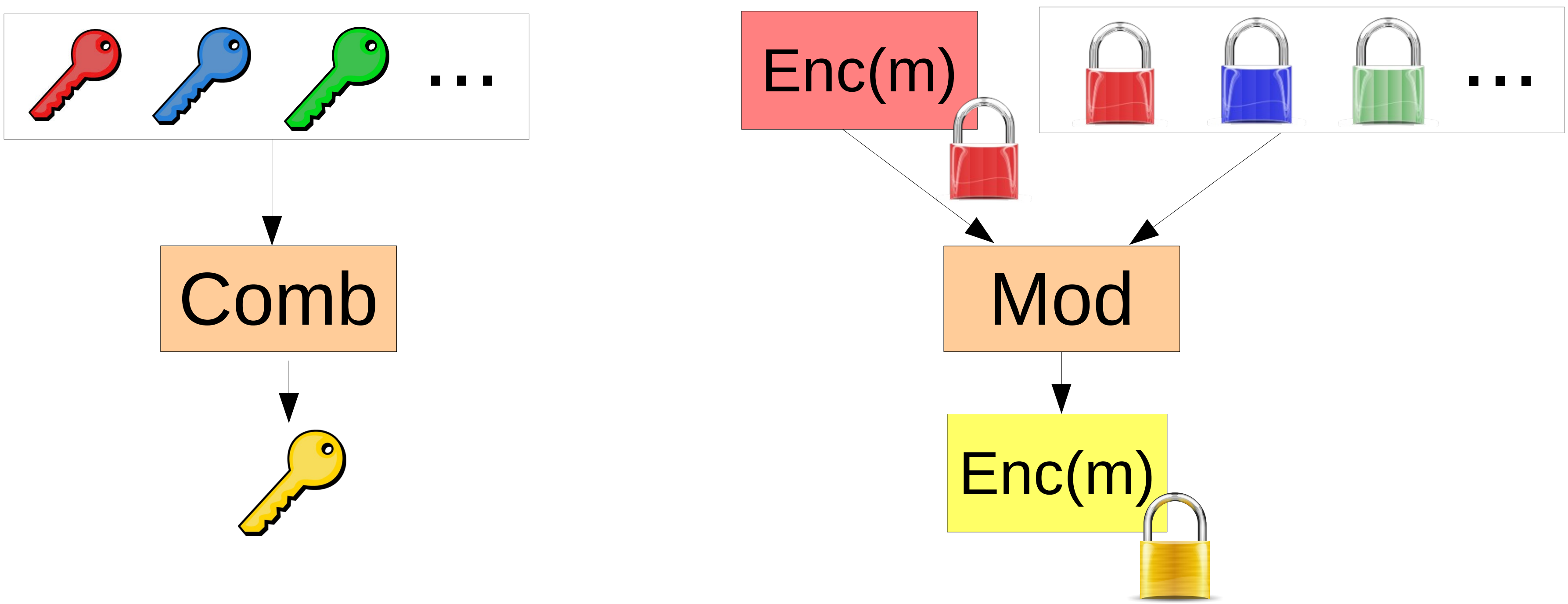
- ElGamal encryption: $(pk, sk) = (g^x, x)$
- $Enc_{pk}(m) = (g^r, (g^x)^r m)$
- homomorphism μ: $g^x \cdot g^y = g^{x+y}$



- $sk_{ID} = \sum_{i \in \varphi(ID)} x_i$
- IBE ciphertext is just a PKE ciphertext
  - 2 group elements!
- Constructions from QR [GLW12], LWE [GPV07]

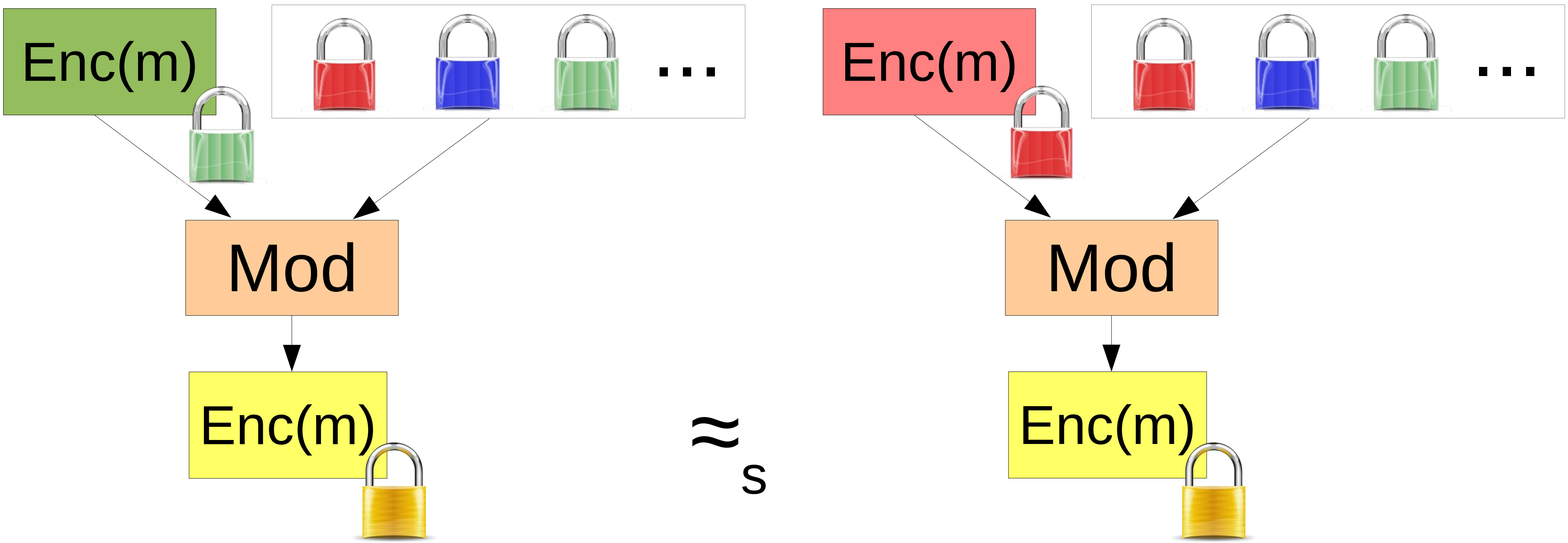
Multi-Key Malleability

- PKE is n-key malleable if ∃ PPT Comb, Mod:



Multi-Key Malleability

- PKE is n-key malleable if ∃ PPT Comb, Mod:



BC-IBE from Multi-Key Malleability

- IBEGen: Run Gen^n
  - $PP = (pk_1,\ldots pk_n)$
  - $msk = (sk_1,\ldots sk_n)$
- IBEExtract:
  - $sk_{ID} = Comb(\varphi(ID), msk)$
- IBEEnc:
  - $i = \min(\varphi(ID))$
  - $c' = Enc(pk_i, m)$
  - $c = Mod(PP, \varphi(ID), c)$

BC-IBE from Multi-Key Malleability

- IBEGen: Run Gen^n
  - PP = $(pk_1, \ldots pk_n)$
  - msk = $(sk_1, \ldots sk_n)$
- IBEExtract:
  - sk_{ID} = Comb(φ(ID), msk)
- IBEEnc:
  - i = min(φ(ID))
  - c' = Enc(pk_i, m)
  - c = Mod(PP, φ(ID), c)

Thm. If PKE is semantically secure and n-key-malleable, and φ is (t+1)-cover-free, then this BC-IBE is (fully) semantically secure.

NTRU

- Consider polynomial ring $R = Z[x]/(x^r+1)$
- χ = distribution over R w/coeffs bounded by B
- $f,g \leftarrow \chi$, $f \equiv 1 \bmod 2$
- sk=f; pk=2g/f (over R_q)
- Enc(pk, b): $h,e \leftarrow \chi$; $c = h \cdot pk + 2e + b$
- Dec(sk, c): Output $sk \cdot c \pmod 2$

NTRU-Based Construction

- Comb: Given:

  $sk_1 \ldots sk_n$

  Return $\prod_i sk_i$

- Mod: Given:

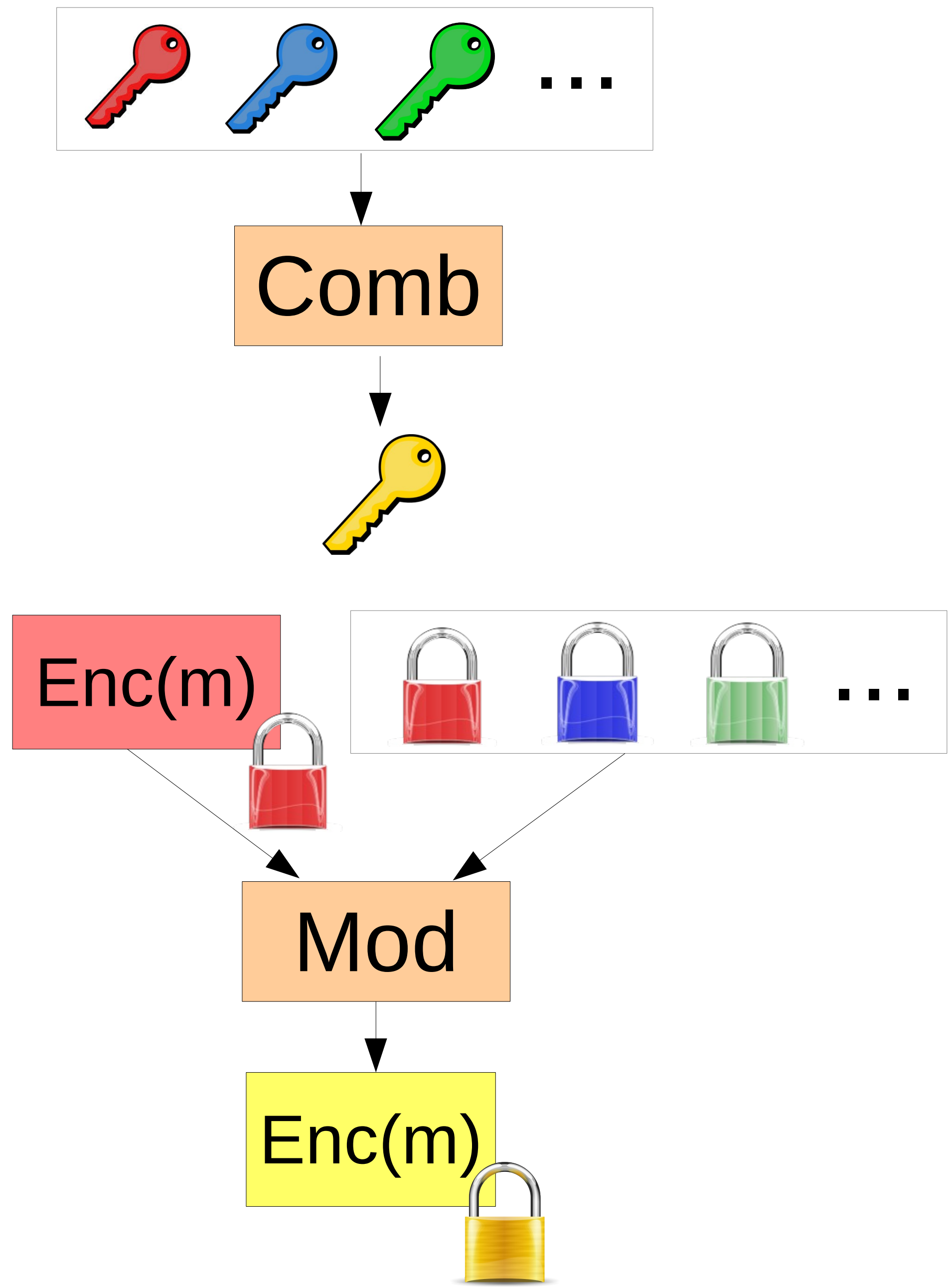
  $c = h\, pk_i + 2e + b$

  $pk_1 \ldots pk_n$

  Sample $h_j \leftarrow \chi \ (j \in [n] \backslash i)$

  Return $c + \sum_{j \in [n] \backslash i} h_j\, pk_j$

  $= \sum_j h_j\, pk_j + 2e + b$



NTRU-Based Construction

- Modified ciphertexts are now of the form

  $\sum_i 2h_i g_i/f_i + 2e + b$

- Combined keys are of the form

  $\prod_j f_j$

- Thus, decryption yields

  $\sum_i 2h_i g_i(\prod_{j\neq i} f_j)) + 2e(\prod_j f_j) + (\prod_j f_j)b \pmod 2$

- We can set parameters q, r, B s.t. this equals b

Bounded-CCA Security

- Any selectively-secure IBE implies a CCA-secure PKE [BCHK07]
- The reduction carries over in the bounded-collusion model; any selectively-secure t-BC-IBE implies a t-bounded CCA PKE.
- GLW construction: semantically-secure PKE with homomorphism → bounded-CCA PKE with same ciphertext size
- bounded-CCA NTRU construction has smaller ciphertexts than any known NTRU-based CCA PKE

Open Problems

- More examples!
- Other properties that yield BC-IBE (possibly with smaller public parameters)

Questions?