Robustness of the Learning with Error (LWE) Assumption

Shafi Goldwasser Weizmann/MIT

Yael Tauman Kalai Microsoft

Chris Peikert Georgia Tech

Vinod Vaikuntanathan IBM

Cryptography

sk

0	1	1	1	0	0

sk

0	1	1	1	0	0

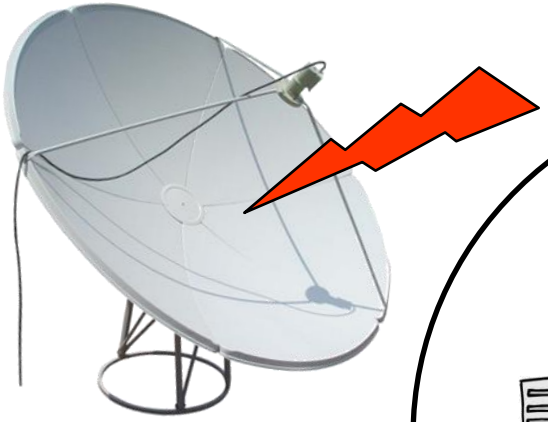
Public-key cryptography (e.g. RSA)

(sk_1, pk_1) (sk_2, pk_2)

RSA (and other schemes) are **insecure** when a small fraction of the secret key is leaked

[Rivest-Shamir85, Coppersmith1996, Heninger-Shacham2009]

Computation Leaks



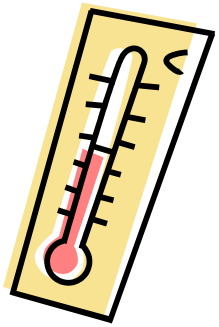
EM Radiation

[Quisquater 01]

Power Consumption

[Kocher et al. 98]

Timing [Kocher 96]



Memory Leaks

Cold-boot attack

[HSHCPCFAF 08]

Benign Leakage

- **Weak keys**
  - Secret keys may not be generated with perfect randomness
- **Re-use of secret keys**
  - We may want to use the same secret key for different applications (i.e., biometrics, identity based crypto,…).

How Do we Deal with These Attacks?

Traditionally:

"this is not our job. We're theorists. Our job is to design schemes that are secure assuming the secret key is totally hidden."

Recently:

Use more theory to battle reality.

Outline

- ✓ **Motivation**
- **Modeling Leakage**
- **Thm:** Learning With Error (LWE [Regev2005]) problem is hard even with leakage
- **Proof overview**
- **Application:** Efficient symmetric encryption scheme robust to leakage

Modeling Leakage

Computation leaks

[Micali-Reyzin2004]
[Ishai-Prabhakaran-Sahai2003]
[Wagner2006]
[Dziembowski-Pietrzak2008]
[Pietrzak2009]
[Faust-Kiltz-Pietrzak-Rothblum2009]

Memory leaks

[Akavia-Goldwasser-Vaikuntanathan2009]
[Dodis-K-Lovett2009]
[Naor-Segev2009]
[Katz-Vaikuntanathan2009]
[Alwen-Dodis-Wichs2009]
[Alwen-Dodis-Naor-Segev-Walfish-Wichs2009]
[Dodis-Goldwasser-K-Peikert-Vaikuntanathan2010]
[Goldwasser-K-Peikert-Vaikuntanathan2010]

Memory Leakage

Goal: Construct schemes (standard) secure w.r.t. leakage

Challenge: Don't strengthen computational assumptions

[Rivest97, Boyko99, Canetti-Dodis-Halevi-Kushilevitz-Sahai00]: Bit leakage

[Akavia-Goldwass

[Naor-Segev2009]:

[Dodis-K-Lovett2009]: sk is ha

given L(sk)

Useful for composition:
Reuse secret key across different applications

on L(sk)

mputationally) to compute

X has min-entropy k if
$\forall x,\ Pr[X=x] \leq 2^{-k}$

Formally: $\forall$ PPT A, $Pr[A(L(sk))=sk] < 2^{-k}$

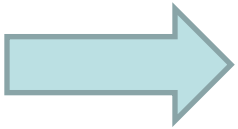
Previous Results

- [Akavia-Goldwasser-Vaikuntanathan2009]: Regev's public-key encryption scheme is secure against leakage.
- [Naor-Segev2009]: several public-key encryption schemes secure against leakage.
- [Katz-Vaikuntanathan2009]: Signature schemes secure against leakage.
- [Dodis-K-Lovett2009]: Symmetric-key encryption scheme secure w.r.t. auxiliary input leakage.
- [Dodis-Goldwasser-K-Peikert-Vaikuntanathan2010]: Several public-key encryption schemes secure w.r.t. auxiliary input leakage.

Drawback

The parameters of the schemes depend on maximum anticipated leakage

Security w.r.t. $(1-\epsilon)$ leakage



$\text{poly}(1/\epsilon)$ efficiency loss

Scheme Independent of Leakage Parameters

This work:

Single symmetric-key encryption scheme, secure against **any** auxiliary input leakage under standard LWE, and assumption degrades proportional to leakage size

same assumption with
smaller security parameter

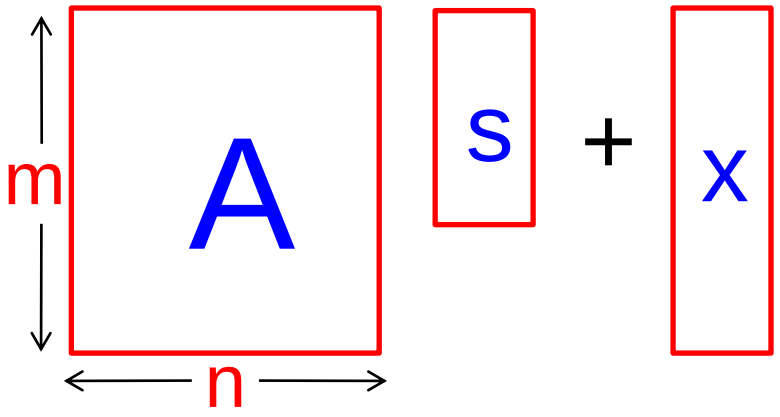
Thm:

The LWE assumption is robust to auxiliary input leakage:
It degrades proportional to leakage size

Learning with Errors (LWE)
[Regev2005]

$LWE_{n,m,q,\chi}$ Assumption: $(A, As+x) \approx (A, U)$

where $s \in_R Z_q^n$, $A \in_R Z_q^{m \times n}$, and $x \leftarrow \chi^m$,



- Decision to search reduction
- Can be reduces to the worst-case hardness of approximating shortest vector in lattice [Regev05,Peikert09]

Usually: χ is "discrete" Gaussian distribution

Robustness of LWE

Thm: $(A, As+x) \approx (A, U)$

where $s \in \{0,1\}^n$ is weak source with min-entropy k,

$A \in_R Z_q^{m \times n}$, $x \leftarrow \chi^m$, and q=super-poly(n),

assuming $\mathbf{LWE}_{k/(\log q),m,q,\chi'}$

std dev is super-poly small

Thm: $(A, As+x) \approx (A, U)$

where $s \in \{0,1\}^n$ is weak source with min-entropy k,

$A \in_R Z_q^{m \times n}$, $x \leftarrow \chi^m$, and q=super-poly(n),

assuming $\mathbf{LWE}_{k/(\log q),m,q,\chi'}$

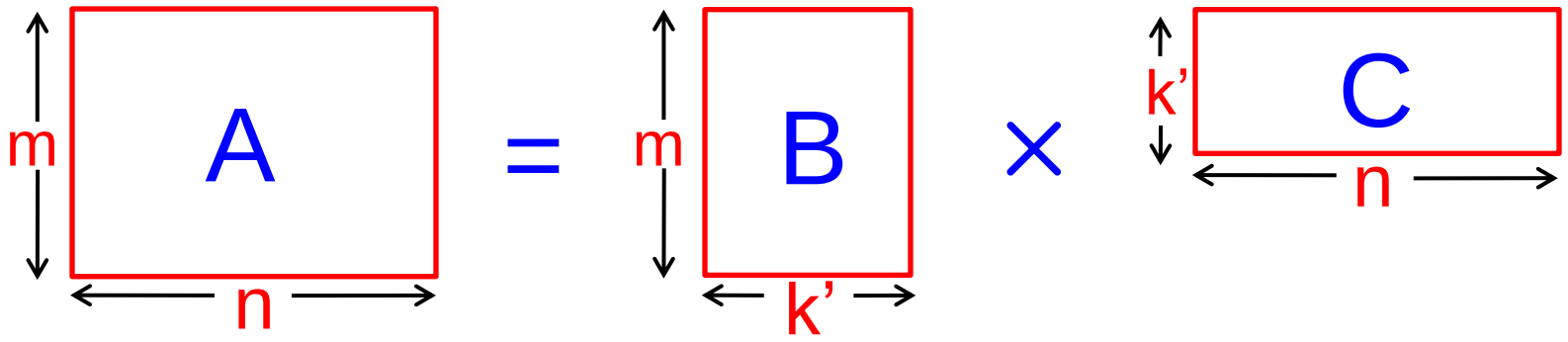
Thm: $(A, As+x) \approx (A, U)$

where $s \in \{0,1\}^n$ is weak source with min-entropy k,

$A \in_R Z_q^{m \times n}$, $x \leftarrow \chi^m$, and q=super-poly(n),

assuming $\mathbf{LWE}_{k/(\log q),m,q,\chi'}$

Proof: Suppose



$$As+x = BCs+x = Bu+x \approx U$$

Leftover hash lemma

$k' < k/\log q$

$\mathbf{LWE}_{k',m,q,\chi}$

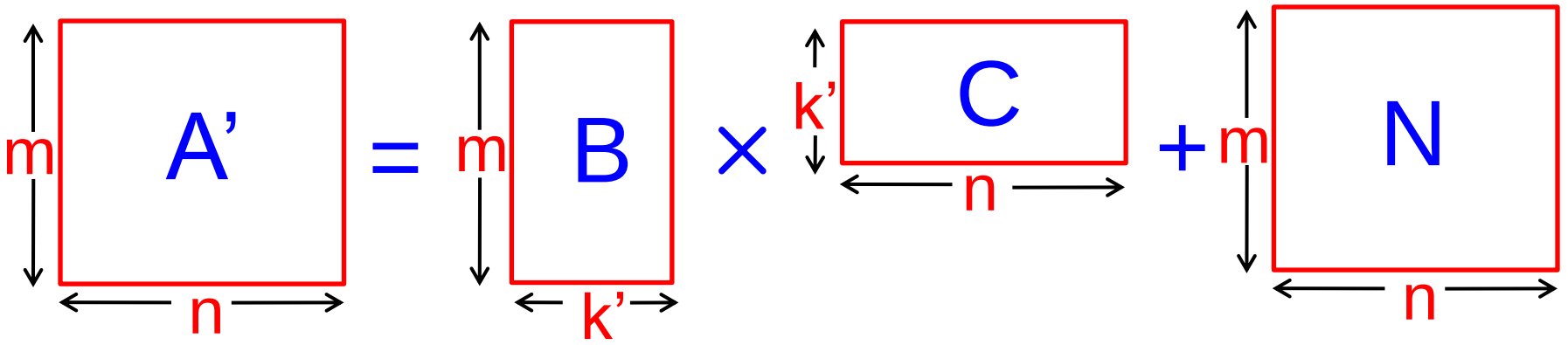
Thm: $(A, As+x) \approx (A, U)$

where $s \in \{0,1\}^n$ is weak source with min-entropy k,

$A \in_R Z_q^{m \times n}$, $x \leftarrow \chi^m$, and q=super-poly(n),

Assuming $\mathbf{LWE_{k/\log,m,q,\chi}}$

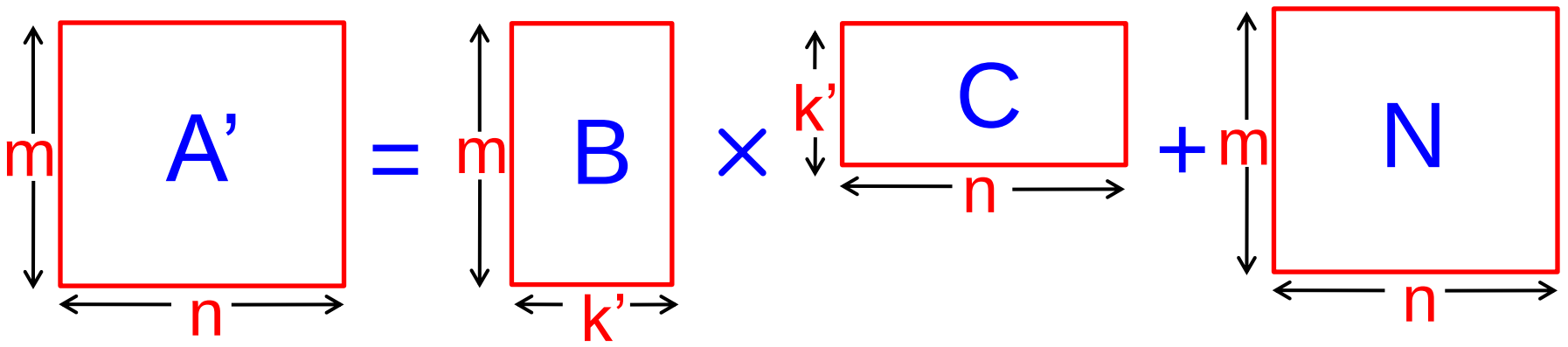
Proof: Let



Claim1: $A' \approx A$ assuming $LWE_{k',m,q,\chi'}$

Claim2: $(A', A's+x) \approx (A', U)$ assuming $LWE_{k',m,q,\chi}$

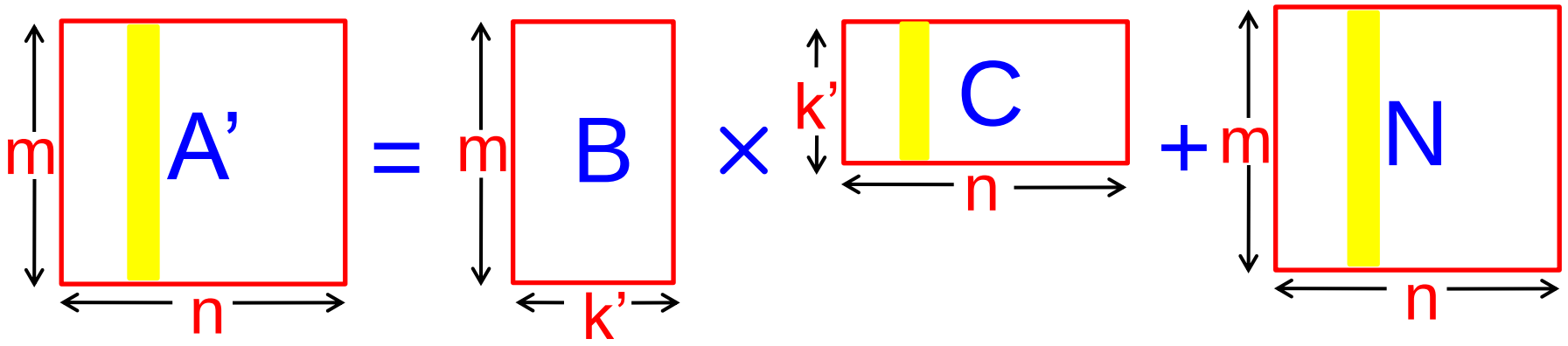
Proof: Let



Claim1: $A' \approx A$ assuming $LWE_{k',m,q,\chi'}$

Claim2: $(A', A's+x) \approx (A', U)$ assuming $LWE_{k',m,q,\chi}$

Proof: Let



Claim1: $A' \approx A$ assuming $LWE_{k',m,q,\chi'}$

Claim2: $(A', A's+x) \approx (A', U)$ assuming $LWE_{k',m,q,\chi}$

$LWE_{k',m,q,\chi}$

$A's+x = (BC+N)s+x = BCs+Ns+x \equiv BCs+x \equiv Bu+x \approx U$

$Ns+x \equiv x$, since $x >> Ns$:
x is Gaussian with std deviation super-poly(n) larger than N

$k' < k/\log q$

■

The Encryption Scheme

Secret key: $s \in_R \{0,1\}^n$

$x \leftarrow \chi^m$ is Gaussian

Enc. Alg: $Enc_s(M) = (A, As+x+(q/2)M))$

— a_1 —

A =

The scheme is **independent** of leakage parameters

Ecc(M)∈ {0,1

Dec. Alg : $Dec_s(A,y) = decode(y-As)$

Summary

Thm: LWE problem is hard even with weak secrets, and hardness decays proportional to leakage

even with auxiliary input

Corollary: Symmetric encryption scheme secure w.r.t. auxiliary input leakage under LWE, where efficiency of the scheme is independent of maximum anticipated leakage.

Corollary [Canetti-K-Mayank-Wich2010]**:** (distributional) obfuscation for point function with multi-bit output under standard LWE.

Thanks !