Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors

N. Kunihiro (The University of Tokyo),
N. Shinohara (NICT) and
T. Izu (Fujitsu Labs.)

Accepted by PKC2013 @Nara, Japan

Motivation:

Situation:

A noisy variant of secret keys are obtained by coldboot attack or side channel attack.

Correct Keys: (p, q, d, d_p, d_q)

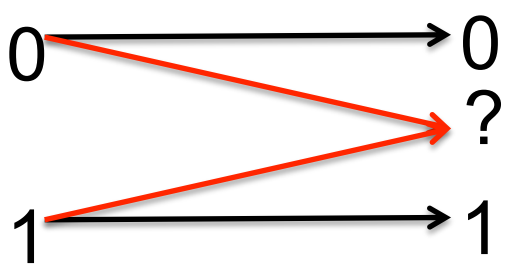
→ Noise Keys (p', q', d', d_p', d_q')

- How to recover the correct keys from the noisy keys?
- What is the condition where we can recover the secret keys in polynomial time?
- And its theoretical bound?

Noise Models

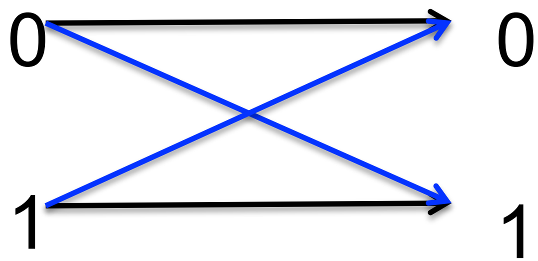
Heninger-Shacham (Crypto2009)

Symmetric Erasure



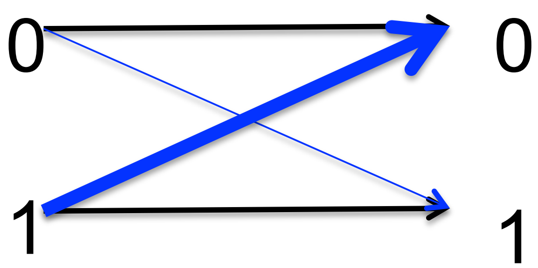
Henecka-May-Meurer (Crypto2010)

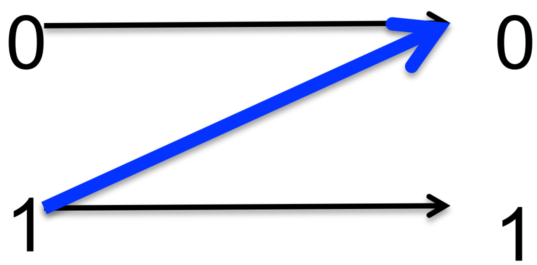
Symmetric Error



Paterson-Polychroniadou-Sibborn(Asiacrypt2012)

Asymmetric Error

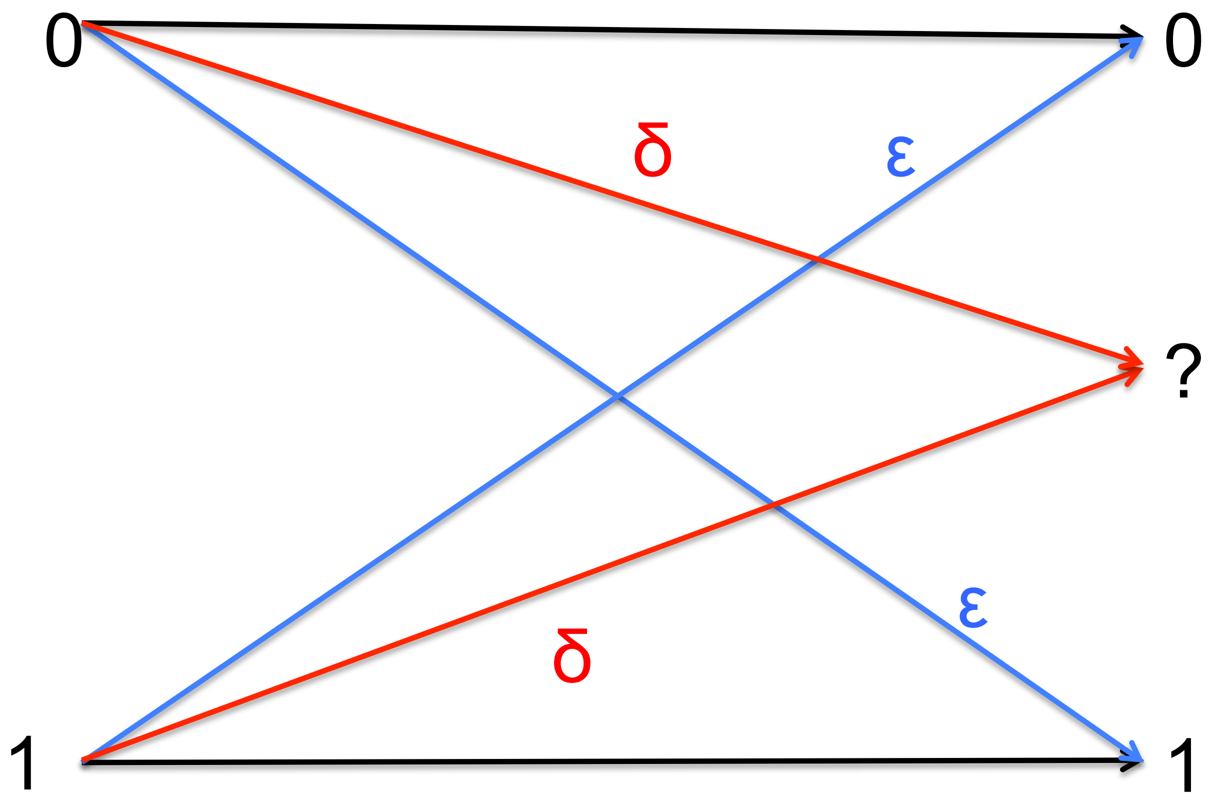




realisitic coldboot attack scenario

Our Noise Model

Symmetric Erasure and Error



Our noise model is appropriate for side-channel attack scenario rather than coldboot attack scenario.

Our Problem (informal)

Each bit of secret key (p, q, d, d_p, d_q)

- is erased with prob. δ or
- is bit-flipped with prob. ε.

We want to recover the correct secret keys from the noisy keys.

We want to know

1. the condition such that we can recover the secret key in polynomial time.
2. the theoretical bounds under the reasonable constrain.

Our Contributions

Contribution1：

If $\varepsilon + \frac{\delta}{2} \leq \frac{1}{2} - \sqrt{\frac{(1-\delta)\ln 2}{10}}$

we can recover the secret keys in polynomial time.

Our bound is equivalent to

- the bound of HS when $\varepsilon = 0$ and
- the bound of HMM when $\delta = 0$.

Our method unifies the HS and HMM methods.

Contributions2：

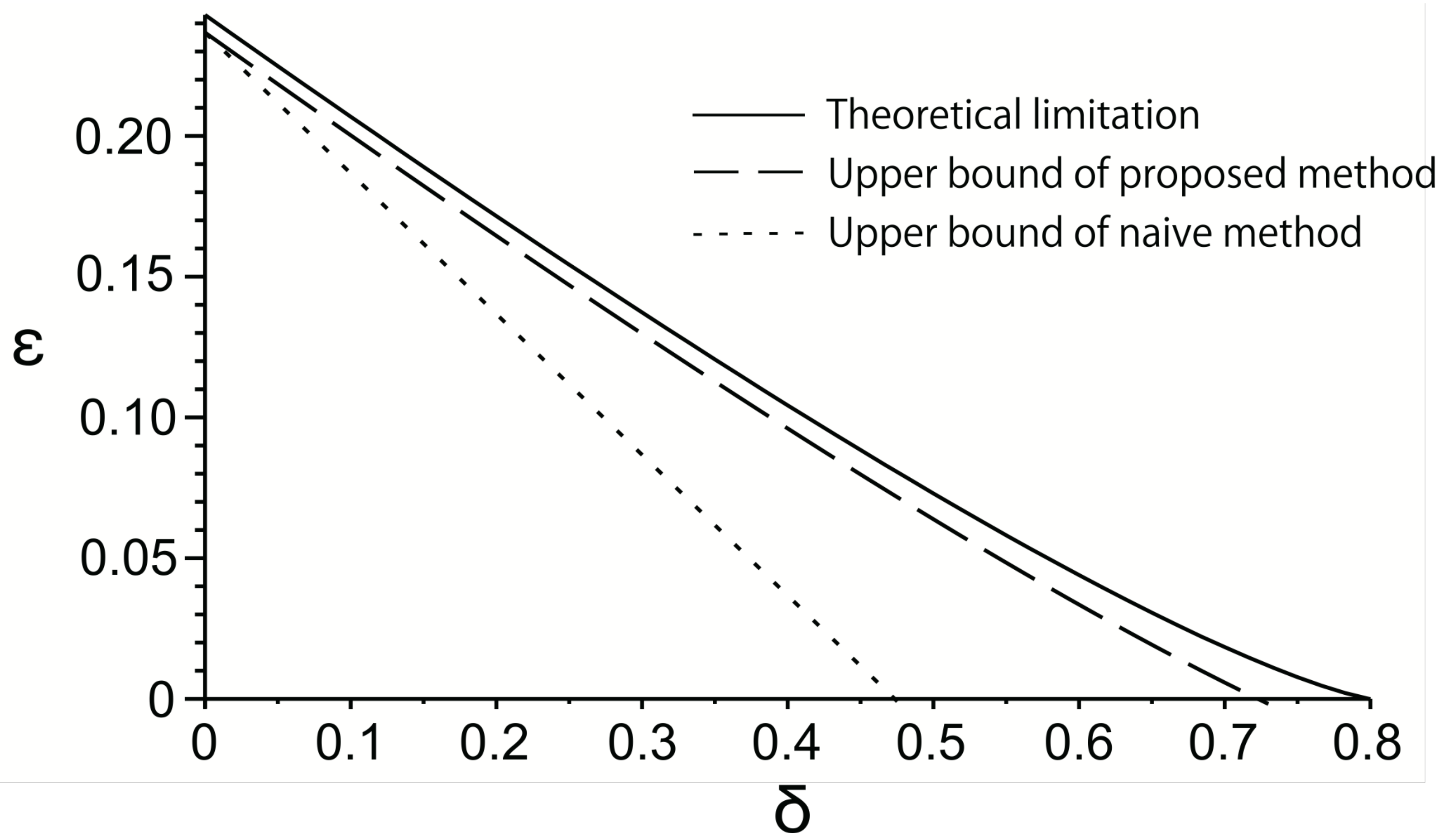
We prove that we cannot recover the correct secret keys in polynomial time if

$$(1-\delta)\left(1-H\left(\frac{\varepsilon}{1-\delta}\right)\right) \geq \frac{1}{5}$$

Channel Capacity of Erasure-Error Channel

information rate

Comparison of our achieved bound and theoretical bound



Almost achieves, but small gap!

Contribution 3

We show a strong relation between two bounds.
By Taylor expansion around x=1/2, we can transform the theoretical bound into

$$(1-\delta)\sum_{t=1}^{\infty}\frac{1}{2t(2t-1)}\left(\frac{1-\delta-2\varepsilon}{1-\delta}\right)^{2t} \geq \frac{\ln 2}{r}.$$

Truncating by t=1, the achieved bound is obtained.
Our algorithm achieves the second order expansion of the theoretical bound.

Thank you!

See you at
PKC2013@Nara, Japan!