On the Circular Security of Bit Encryption

Ron Rothblum
Weizmann Institute

Circular Security

An encryption scheme is circular secure if it is "safe" to encrypt the decryption-key.

Def: [CL01,BRS02] a public-key scheme is circular secure if for every PPT A,

$$|\Pr[A^{Enc_e(d)}(e) = 1] - \Pr[A^{Enc_e(0^{|d|})}(e) = 1]|$$

is negligible.

Circular Security

Q: Is it in general safe to encrypt your own key?

A: For some schemes (e.g. [BHHO08,ACPS09]) yes but in general **No!**

Circular Security

Easy counterexample: given semantically secure private-key encryption (Enc, Dec):

$$Enc'_k(m): \quad \begin{array}{l} \text{if } k = m \text{ output } k \\ \text{else output } Enc_k(m) \end{array}$$

Can be extended to public-key.

Public Key Example

The encryption algorithm can test if the message m functions as a “good” decryption-key by using it to decrypt many random messages.

Circular Security of Bit Encryption

Since general case is false, focus on interesting special case of *bit-encryption*.

Messages are encrypted bit-by-bit:
$Enc_e(\sigma_1, \ldots, \sigma_t) = Enc_e(\sigma_1), \ldots, Enc_e(\sigma_t)$

Why bit-encryption?

1. Most candidate FHE are bit-encryption whose semantic-security relies on their circular security (which is not understood).
2. Seems most natural way to foil the previous counterexample and get circular security for "free".

Bit-Encryption Conjecture

Conjecture: [Folklore]

Every semantically-secure bit-encryption scheme is circular secure.

Focus of this work is showing obstacles to proving the conjecture.

Our Results

1. A scheme that is circular **insecure** but is semantically secure based on multilinear maps.
2. Cannot prove the conjecture via a blackbox reduction.
3. Equivalence of different security notions for circular security of bit-encryption.

Our Results

1. A scheme that is circular **insecure** but is semantically secure based on multilinear maps.
2. Cannot prove the conjecture via a blackbox reduction.
3. Equivalence of different security notions for circular security of bit-encryption.

Our Assumption

An extension of an assumption made on groups with bilinear maps to groups with multilinear maps.

Multilinear Maps

Let $G_1, \dots, G_\ell$ and G_T be cyclic groups of prime order p.

An ℓ-linear map is a (non-degenerate) function

$$e: G_1 \times \cdots \times G_\ell \to G_T$$

such that **for every $\boldsymbol{i} \in [\ell]$**

$$e(g_1, .., g_i^a, \dots, g_\ell) = e(g_1, \dots, g_\ell)^a$$

where $g_1 \in G_1, \dots, g_\ell \in G_\ell$ and $a \in \{0, \dots, p-1\}$.

Multilinear Maps

There exist trivial multilinear maps unconditionally but for crypto, need computational problems such as discrete-log to be hard.

Do there exist multilinear groups on which discrete-log (and friends) are hard? [BS03]

(Silly) Example

Consider $G_1 = \cdots = G_\ell = Z_p^+$.

Exponentiation in these groups corresponds to multiplication modulo p.

Consider:

$$e(x_1, \ldots, x_\ell) = \prod_{i \in [\ell]} x_i \mod p$$

But discrete-log is easy in these groups!

SXDH Assumption [BGMM05, ACHM05]

There exists a bilinear (aka 2-linear) map where DDH is hard in both G_1 and G_2.

DDH in group G:

$$\left(g, g^a, g^b, g^{ab}\right) \stackrel{c}{=} \left(g, g^a, g^b, g^c\right)$$

For gen g $\in G$ and $a, b, c \in_R \{0, \ldots, p-1\}$

Exist concrete candidates (elliptic curves) on which SXDH is conjectured to hold.

Previously used for counterexample for 2-cycle security of general encryption [ABBC10, CGH12].

ℓ-multilinear SXDH Assumption

There exists an ℓ-multilinear map where DDH is hard in all groups $G_1, .., G_\ell$.

Until recently, no concrete cand
$\ell = 3$.

p is the group order
n is the security parameter

[GGH13] give a lattice-based candidate (approximate) ℓ-linear map for $\ell < \frac{\log p}{n^2}$.

Approximate is fine for us but ℓ is not large enough.

Theorem

If the ℓ-linear SXDH assumption holds for $\ell > 2\log p$ then there exists a semantically secure bit-encryption scheme that is not circular secure.

$\Rightarrow$ Either the bit-encryption conjecture is false or the SXDH assumption is easy on **all** ℓ-multilinear groups.

Our construction is based on ℓ parallel encryptions of an El-Gamal variant + a twist that breaks **circular security** but not **semantic security**.

El-Gamal Variant

Fix group G of order p for which DDH is hard and generator g.

Key Generation:

1. $x_0, x_1 \in_R Z_p$
2. $u_0 = g^{x_0}$ and $u_1 = g^{x_1}$
3. Public-key is (u_0, u_1) and private-key is (x_0, x_1)

Encrypt(σ):

1. $r \in_R Z_p$
2. Output $(g^r, (u_\sigma)^r)$

Decrypt(c,d):

1. If $c^{x_0} = d$ output 0 else output 1

Our Scheme

Fix $G_1, \dots, G_\ell$ of order p for which DDH is hard and gens $g_1, \dots, g_\ell$.

Key Generation:

1. $X = \begin{bmatrix} X[0,1] & X[0,2] & \dots & X[0,\ell] \\ X[1,1] & X[1,2] & \dots & X[1,\ell] \end{bmatrix} \in_R Z_p^{2\times\ell}$

2. $U = \begin{bmatrix} g_1^{X[0,1]} & g_2^{X[0,2]} & \dots & g_\ell^{X[0,\ell]} \\ g_1^{X[1,1]} & g_2^{X[1,2]} & \dots & g_\ell^{X[1,\ell]} \end{bmatrix}$

3. Public-key is U and private-key is X.

Encrypt(σ):

1. $r_1, \dots, r_\ell \in_R Z_p$

2. Output $((g^{r_1}, (U[\sigma, 1])^{r_1}), \dots, (g^{r_\ell}, (U[\sigma, \ell])^{r_\ell})$

Our Scheme

Fix $G_1, \ldots, G_\ell$ of order p for which DDH is hard and gens $g_1, \ldots, g_\ell$.

Key Generation:

1. $X = \begin{bmatrix} X[0,1] & X[0,2] & \ldots & X[0,\ell] \\ X[1,1] & X[1,2] & \ldots & X[1,\ell] \end{bmatrix} \in_R Z_p^{2\times\ell}$

2. $U = \begin{bmatrix} g_1^{X[0,1]} & g_2^{X[0,2]} & \ldots & g_\ell^{X[0,\ell]} \\ g_1^{X[1,1]} & g_2^{X[1,2]} & \ldots & g_\ell^{X[1,\ell]} \end{bmatrix}$

3. Select $s \in_R \{0,1\}^\ell$ and set $\alpha = \sum_{i\in[\ell]} X[s_i, i] \bmod p$

4. Public-key is (U, α) and private-key is (X, s)

Encrypt(σ):

1. $r_1, \ldots, r_\ell \in_R Z_p$

2. Output $((g^{r_1}, (U[\sigma, 1])^{r_1}), \ldots, (g^{r_\ell}, (U[\sigma, \ell])^{r_\ell})$

Circular Security Attack

Get encryptions of bits $b_1, \ldots, b_\ell$ which are either $s_1, \ldots, s_\ell$ or all 0's.

$Enc(b_1)$:	$g_1^{r_{1,1}}, (U[b_1, 1])^{r_{1,1}}$	$g_2^{r_{1,2}}, (U[b_1, 2])^{r_{1,2}}$	…	$g_\ell^{r_{1,\ell}}, (U[b_1, \ell])^{r_{1,\ell}}$
$Enc(b_2)$:	$g_1^{r_{2,1}}, (U[b_2, 1])^{r_{2,1}}$	$g_2^{r_{2,2}}, (U[b_2, 2])^{r_{2,2}}$	…	$g_\ell^{r_{2,\ell}}, (U[b_2, \ell])^{r_{2,\ell}}$
	…	…	…	…
$Enc(b_\ell)$:	$g_1^{r_{\ell,1}}, (U[b_\ell, 1])^{r_{\ell,1}}$	$g_2^{r_{\ell,2}}, (U[b_\ell, 2])^{r_{\ell,2}}$	…	$g_\ell^{r_{\ell,\ell}}, (U[b_\ell, \ell])^{r_{\ell,\ell}}$

Circular Security Attack

$g_1^{r_{1,1}}$	$(U[b_1, 1])^{r_{1,1}}$
$g_2^{r_{2,2}}$	$(U[b_2, 2])^{r_{2,2}}$
….	…
$g_\ell^{r_{\ell,\ell}}$	$(U[b_\ell, \ell])^{r_{\ell,\ell}}$

Circular Security Attack

$g_1^{r_{1,1}}$	$\left(g_1^{X[b_1,1]}\right)^{r_{1,1}}$
$g_2^{r_{2,2}}$	$\left(g_2^{X[b_2,2]}\right)^{r_{2,2}}$
....	...
$g_\ell^{r_{\ell,\ell}}$	$\left(g_\ell^{X[b_\ell,\ell]}\right)^{r_{\ell,\ell}}$

$$y_1 \stackrel{\text{def}}{=} e\left(g_1^{X[b_1,1]\cdot r_{1,1}}, g_2^{r_{2,2}}, \ldots, g_\ell^{r_{\ell,\ell}}\right)$$

Circular Security Attack

$g_1^{r_{1,1}}$	$\left(g_1^{X[b_1,1]}\right)^{r_{1,1}}$
$g_2^{r_{2,2}}$	$\left(g_2^{X[b_2,2]}\right)^{r_{2,2}}$
….	…
$g_\ell^{r_{\ell,\ell}}$	$\left(g_\ell^{X[b_\ell,\ell]}\right)^{r_{\ell,\ell}}$

$$y_i \stackrel{\text{def}}{=} e\left(g_1^{r_{1,1}}, \dots, g_i^{X[b_i,i]\cdot r_{i,i}}, \dots, g_\ell^{r_{\ell,\ell}}\right)$$

Circular Security Attack

If we multiply the y_i's we obtain:

$$\prod_{i\in[\ell]} y_i = \prod_{i\in[\ell]} e\left(g_1^{r_{1,1}}, g_2^{r_{2,2}}, \dots, g_\ell^{r_{\ell,\ell}}\right)^{X[b_i,i]}$$

If $b_i = s_i$ then

$$\prod_{i\in[\ell]} y_i = e\left(g_1^{r_{1,1}}, g_2^{r_{2,2}}, \dots, g_\ell^{r_{\ell,\ell}}\right)^{\sum_{i\in[\ell]} X[s_i,i]}$$

With overwhelming probability

If $b_i = 0$ then

$$\prod_{i\in[\ell]} y_i = e\left(g_1^{r_{1,1}}, g_2^{r_{2,2}}, \dots, g_\ell^{r_{\ell,\ell}}\right)^{\sum_{i\in[\ell]} X[0,i]}$$

$\Rightarrow$ a distinguisher!

Our Results

1. A scheme that is circular **insecure** but is semantically secure based on multilinear maps.
2. Cannot prove the conjecture via a blackbox reduction.
3. Equivalence of different security notions for circular security of bit-encryption.

Blackbox Impossibility Result

No blackbox reduction from circular-security of bit-encryption scheme to semantic-security (or even CCA security) of the **same** scheme.

Blackbox access to encryption-scheme and adversary.

Incomparable to [HH09] KDM blackbox separation.

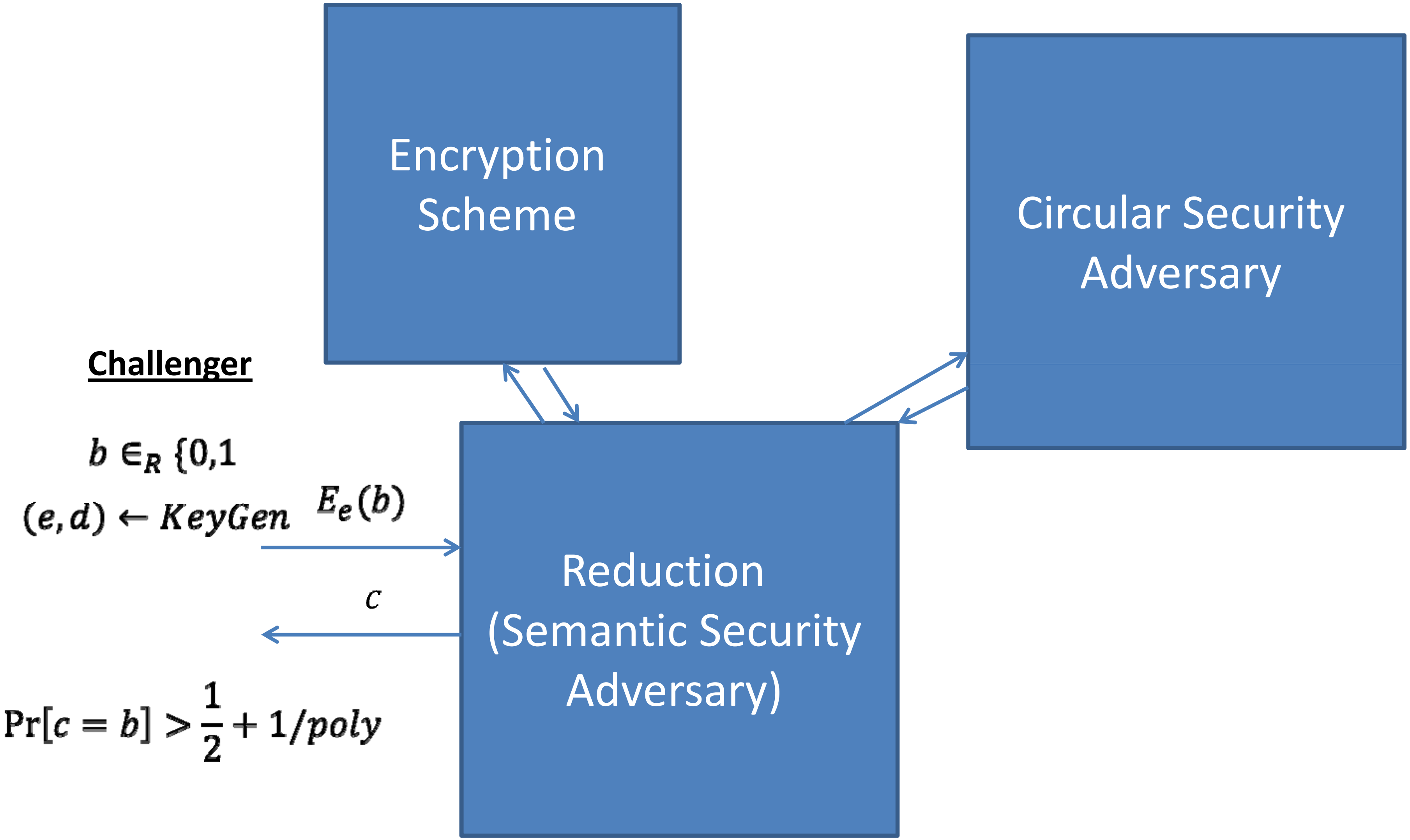
[HH09] KDM Blackbox Impossibility

Two results:

1. No fully blackbox reduction from TDP to KDM security that contains a class of $\mathrm{poly}(n)$-wise independent hash functions.

2. No fully blackbox reduction from essentially any crypto primitive to KDM security if reduction uses the KDM function as a blackbox.

A Blackbox Reduction



Our Results

1. A scheme that is circular <u>**insecure**</u> but is semantically secure based on multilinear maps.
2. Cannot prove the conjecture via a blackbox reduction.
3. Equivalence of different security notions for circular security of bit-encryption.

Circular Security Definitions

Def 1: [CL01,BRS02] a public-key scheme is circular secure if for every PPT A,

$$|\Pr[A^{Enc_e(d)}(e) = 1] - \Pr[A^{Enc_e(0^{|d|})}(e) = 1]|$$

is negligible.

Def 2: a public-key scheme is circular secure **wrt key-recovery** if for every PPT A,

$$\Pr[A^{Enc_e(d)}(e) = d]$$

is negligible.

Equivalence Result

For bit encryption:

Circular-security **distinguisher** $\Rightarrow$ circular-security **key-recovery**.

Corollary 1: a key-recovery adversary for the previous counterexample.

Corollary 2: for current candidate FHE, breaking semantic-security $\Rightarrow$ key-recovery (because oracle can be implemented for free).

Open Problems

1. Show a circular-security attack against any known bit-encryption scheme.

2. Prove circular security or show an attack on any of the candidate FHE.

3. Extend [GGH13] for $\ell > 2 \log p$ or construct a counterexample under a nicer assumption (ideally from the existence of semantically secure encryption).

Thank you!