On Generic Constructions of Circularly-Secure, Leakage-Resilient Public-Key Encryption Schemes

Mohammad Hajiabadi, Bruce Kapron, Venkatesh Srinivasan

March 8, 2016

Background

Circular security for bit-encryption(G, E, D):

- $(pk, sk) \leftarrow G$
- $E_{pk}(sk), E_{pk}(sk), \cdots \equiv^c E_{pk}(0^{|sk|}), E_{pk}(0^{|sk|}), \cdots.$
- This is called bit 1-circular security.
- n-circular security: over n pairs of keys.

Why care about bit 1-circular security

Fundamental notion:

- fully-homomorphic encryption: bootstrappable homomorphic encryption+bit circular security $\Rightarrow$ fully-homomorphic encryption [Gen09]
- Applebaum (Eurocrypt '11): 1-projection security sufficient for F-KDM security for any fixed but arbitrarily-large F.
    - We can also obtain n-projection security. Not discussed in this talk.

leakage-resilient encryption: bounded-memory model, AGV'09

λ-leakage resilient scheme: (G, E, D)

- $(pk, sk) \leftarrow G(1^n)$;
- $f \leftarrow \mathcal{A}(pk)$, s.t. $|f(sk)| \leq \lambda$;
- $\mathcal{A}$ is given $f(sk)$
- $\mathcal{A}$ cannot distinguish between $E_{pk}(0)$ and $E_{pk}(1)$.

r-rate leakage resilient: (G, E, D) is $r \times |sk|$-leakage resilient.

Previous work

- Boneh et al (BHHO'08): BHHO scheme: circular secure under DDH. (proved to be 1-o(1)-rate leakage resilient by [NS '09])
- Brakerski-Goldwasser (BG '10) BG: circular secure and $1 - o(1)$-rate leakage-resilient under Quadratic residuosity (QR) and related (e.g., DCR) assumptions
- bit-CPA security $\not\Rightarrow$ bit-circular security ([Rothblum'13] based on SXDH-hard multilinear maps, [KRW'15] based on indistinguishability obfuscation)

Reproducibility [BBS'03]

Assume $\mathcal{E} = (G, E, D)$ is a private-key encryption scheme.

- We call $\mathcal{E}$ reproducible if for every k_1, k_2, r:
  - $(E_{k_1}(m_1; r), k_2, m_2) \Rightarrow^{\text{Alg } R} E_{k_2}(m_2; r)$.
  - Example: E gives the randomness in the clear (e.g., PRF-based constructions). $E_k(m_1; r) = (r, F_k(r) + m_1)$

Strong (additive) homomorphism

$\mathcal{E} = (G, E, D)$: private-key encryption scheme.

- both plaintext space $(\mathcal{M}, +_m)$ and randomness space $(\mathcal{R}, +_r)$ form groups.
- We have $Hom(E_k(m_1; r_1), E_k(m_2; r_2)) = E_k(m_1 +_m m_2; r_1 +_r r_2)$.

Basic construction

(G, E, D): private-key reproducible, homomorphic bit encryption .
We construct public-key (Gen, Enc, Dec)

- $\mathbf{s} \leftarrow \{0,1\}^\ell$ and
  $\mathbf{p} = (E_k(0; r_1), \ldots, E_k(0; r_\ell), E_k(0; \underbrace{\mathbf{s} \cdot (r_1, \ldots, r_\ell)}_{r_{\ell+1}}))$
- $Enc_{\mathbf{p}}(b)$: return $(E_{k'}(0; r_1), \ldots, E_{k'}(0; r_\ell), E_{k'}(b; r_{\ell+1}))$: can be done using reproducibility.
- $Dec_{\mathbf{s}}(c_1, \ldots, c_\ell, c_{\ell+1})$: return 0 if $Hom_{\mathbf{s}}(c_1, \ldots, c_\ell) = c_{\ell+1}$. Otherwise, return 1.

$Hom_{\mathbf{s}}(c_1, \ldots, c_\ell) = Hom(c_{i_1}, \ldots, c_{i_r})$, where $< i_1, \ldots, i_r >$ are the indices of nonzero bits in $\mathbf{s}$.

Homomorphic weak PRFs

We call $\{F_k\}_{k \in \mathcal{K}} : D \to R$ homomorphic if D and R form groups and $F_k(d_1 + d_2) = F_k(d_1) + F_k(d_2)$.

- A pseudorandom function cannot be homomorphic. Query on d_1, d_2 and $d_1 + d_2$.
- We work with weak pseudorandom functions (NR'95): $(d_1, F_k(d_1)), \dots, (d_p, F_k(d_p))$ is pseudorandom for random $d_1, \dots, d_p$.
- $\{F_k\}$ is called a weak homomorphic PRF if it is weakly pseudorandom and homomorphic.

From HPRF to homomorphic reproducible encryption

F_k is a homomorphic weak PRF. Define $E_k(m; d) = (d, F_k(d) + m)$:

- E is semantically-secure.
- E is homomorphic: $\underbrace{(d_1, F_k(d_1) + m_1)}_{E_k(m_1;d_1)}, \underbrace{(d_1, F_k(d_2) + m_2)}_{E_k(m_2;d_2)} \Rightarrow$ $\underbrace{(d_1 + d_2, F_k(d_1 + d_2) + m_1 + m_2)}_{E_k(m_1+m_2;d_1+d_2)}$.
- E is reproducible: randomness is given in the clear.

Constructing weak homomorphic PRFs

We show a DDH-based construction.

- Define $F_k : G \mapsto G$ for $k \in \mathbb{Z}_{|G|}$ as $F_k(q) = q^k$.
- F_k is homomorphic: $F_k(q_1 \cdot q_2) = F_k(q_1) \cdot F_k(q_2)$.
- Weak pseudorandomness: $\mathcal{DS}_1 \equiv^c \mathcal{DS}_2$, where

$$\mathcal{DS}_1 = \begin{pmatrix} g_1 & \cdots & g_\ell \\ g_1^k & \cdots & g_\ell^k \end{pmatrix} \tag{1}$$

$$\mathcal{DS}_2 = \begin{pmatrix} g_1 & \cdots & g_\ell \\ g_l' & \cdots & g_\ell' \end{pmatrix} \tag{2}$$

follows using random-self-reducibility of DDH (Naor-Reingold, Boneh et al).

- We can realize a homomorphic weak PRF using a homomorphic hash-proof-system (CS'02)–See paper.
- Also show constructions of reproducible, PR-homomorphic encryption based on QR, DCR.
- We also prove *auxiliary-input security* ([DGKPV'10]) against *sub-exponentially-hard functions* for the constructed scheme.

Open questions

- More general assumptions?
- Applicability to LWE (and related) assumptions? (Applebaum et al (Crypto 09) give an LWE-based circular-secure scheme).

Thanks!