Cryptanalysis of the Quadratic Zero-Testing of GGH[*]

Zvika Brakerski[†]
Weizmann Institute of Science

Craig Gentry
IBM

Shai Halevi
IBM

Tancrède Lepoint[‡]
CryptoExperts

Amit Sahai[§]
UCLA

Mehdi Tibouchi
NTT Secure Platform Laboratories

August 31, 2015

Abstract

In this short note, we analyze the security of the quadratic zero-testing procedure for the GGH13 graded encoding scheme, which was recently proposed by Gentry, Halevi and Lepoint. We show that this modification fails to immunize the GGH13 construction against zeroizing attacks, and that the modified scheme is susceptible to the same attacks as the original one.

1 Introduction

Zeroizing attacks [GGH13a, CHL+15, CGH+15, HJ15] were shown to be a potent line of attacks against existing graded encoding candidates [GGH13a, CLT13, GGH15]. Although many applications do not seem to be affected by these attacks (most notably indistinguishability obfuscation [GGH+13b]), these attacks were used to break a number of applications (and many hardness assumptions on) these graded encoding candidates.

Roughly speaking, zeroizing attacks proceed by honestly computing many top-level encoding of zero, then using the prescribed zero-testing procedure to setup and solve a system of multilinear equations in the secret parameters of the scheme. These attacks rely crucially on the linearity of the zero-testing procedure, and so some attempts were made recently to devise alternative zero-testing procedures that are non-linear. In one of these attempts [Hal15], Gentry, Halevi and Lepoint recently described a variant of the GGH13 candidate scheme [GGH13a], in which the linear zero-testing procedure from [GGH13a] is replaced by a quadratic (or higher-degree) procedure.

Our Work. In this short note, we show that the Gentry-Halevi-Lepoint (GHL) variant remains susceptible to the same zeroizing attacks as the original GGH13. In particular, we show how to construct a native GGH13 zero-test parameter from the GHL quadratic zero-test parameter. In a nutshell, this is done by computing the "derivative" of the quadratic zero-test polynomial at a top-level encoding of zero, thus obtaining a linear zero-test polynomial that can be transformed into a native GGH13 zero-test parameter.

2 GGH with High-Degree Zero-Test

The GGH13 graded encoding candidate [GGH13a] works over the quotient ring $R_q = R/qR$ where $R = \mathbb{Z}[x]/(x^n + 1)$ is the $2n$-th cyclotomic polynomial ring (n a power of two) and q is a large modulus.[1] The plaintext space is $R_g = R/gR$ where $g \in R$ is a small (secret) element. A level-k encoding u of $m \in R_g$ is such that $u = [c/z^k]_q$ where $c \in m + gR$ is small and $z \leftarrow R_q$ is a random (secret) multiplicative mask. Encodings at the same levels can be added (and the encoded values get added modulo R_g), and encodings can be multiplied as long as the sum of the levels remains smaller than the multi-linearity level κ (and the encoded values get multiplied modulo R_g).

The GGH13 Zero-Testing. The zero-testing procedure of GGH13 consists in multiplying a level-κ encoding $u = [c/z^\kappa]_q$ by a public value $p_{zt} = [h/g \cdot z^\kappa]_q$, where h is a somewhat small secret value, so that

$$w = [u \cdot p_{zt}]_q = [h \cdot (c/g)]_q \tag{1}$$

has norm smaller than (say) $q^{3/4}$ if and only if $c \in gR$, i.e. if and only if u is a top-level encoding of $0 \in R_g$. Now when $c = gr$ over R, Eq. (1) holds over R and gives $w = h \cdot r$ which is linear in r. This R-linearity can then be exploited in zeroizing attacks [GGH13a, HJ15].

Quadratic Zero-Testing. During the invited talk of CRYPTO 2015, Halevi described a tentative fix due to Gentry, Halevi and Lepoint (GHL) aiming at making the zero-testing procedure at least quadratic in the coefficients of the input (and therefore breaking the R-linearity of the zero-testing procedure at the core of the zeroizing attacks) [Hal15]. For any encoding $u = \sum_{i=0}^{n-1} u_i \cdot x^i \in R_q$, denote $\vec{u} = (u_0, \ldots, u_{n-1}) \in \mathbb{Z}_q^n$ its vector of coefficients. The GHL zero-testing procedure is given by a quadratic polynomial $p \colon \mathbb{Z}_q^n \to \mathbb{Z}_q$ such that

$$|p(\vec{u}) \bmod q| < q^{3/4} \iff u \text{ is a top-level encoding of } 0 \,.$$

The key idea is to define p as $p(\vec{u}) = \sum_{i,j} \alpha_{ij} \cdot \ell_i(\vec{u}) \cdot \ell_j(\vec{u})$ where the $\alpha_{i,j}$'s are small (say, $\|\alpha_{ij}\|_\infty < q^{1/4}$) and the ℓ_i's are the linear equations corresponding to the multiplication by a native GGH13 zero-test parameter p_{zt} over R_q, i.e. such that $w = [u \cdot p_{zt}]_q$ has coefficient-vector $\vec{w} = (\ell_0(\vec{u}), \ldots, \ell_{n-1}(\vec{u}))$ and (say) $\|w\|_\infty < q^{1/4}$.

Extension to Higher Degrees. It is easy to generalize the GHL zero-testing procedure to a polynomial of higher degree d as follows [Hal15]:

$$p(\vec{u}) = \sum_{i_1, i_2, \ldots, i_d} \alpha_{\vec{i}} \cdot \ell_{i_1}(\vec{u}) \cdots \ell_{i_d}(\vec{u}) \,.$$

---

[1] Our attack extends to any cyclotomic polynomial ring $R = \mathbb{Z}[x]/(\Phi(x))$ when Φ has small enough coefficients. For ease of simplicity we restrict our description to $\Phi(x) = x^n + 1$ for n a power of 2.

Note, however, that describing the new zero-test polynomial takes $\Theta(n^d)$ terms, hence for this zero-test procedure to be polynomial-time we need the degree d to be a constant.

3 Cryptanalysis

The key idea of the attack will be to compute the "derivative" of the high-degree polynomial in a top-level encoding of 0, reducing its degree until we get back a linear polynomial.

Definition. Let $p(x_0, \ldots, x_{n-1}) \in \mathbb{Z}_q[x_0, \ldots, x_{n-1}]$ be a polynomial. For all $\vec{a} = (a_1, \ldots, a_{n-1}) \in \mathbb{Z}_q^n$, we define $p'_{\vec{a}} \in \mathbb{Z}_q[x_1, \ldots, x_n]$ the derivative of p in $\vec{a}$ as

$$p'_{\vec{a}}(x_0, \ldots, x_{n-1}) = p(x_0 + a_0, \ldots, x_{n-1} + a_{n-1}) - p(x_0, \ldots, x_{n-1}) \bmod q.$$

Remark. Note that if $p(\vec{x})$ is of total degree $t \geq 1$ in the x_i's, then $p'_{\vec{a}}(\vec{x})$ is of total degree at most $t - 1$.

The attack consists of three parts: We first compute the $d-1$'st derivative of the given degree-d zero test, thus obtaining an affine zero-test polynomial, then we observe that the free term of this affine polynomial must be small and can be ignored, and finally we show how to recover a native GGH13 zero-test parameter from the resulting linear zero-test.

Step 1: Reducing the Degree

Let $p_d(\cdot)$ be the degree-d zero-testing polynomial of GHL, so for every top-level encoding of zero x we have $|p_d(\vec{x}) \bmod q| < q^{3/4}$ (say). Also let $u \in R_q$ be some fixed top-level encoding of zero. For $i = 1, 2, \ldots, d-1$ we compute $p_{d-i}(\cdot)$ by deriving $p_{d+1-i}(\cdot)$ at u, setting

$$p_{d-i}(\vec{x}) = p_{d+1-i}(\vec{x} + \vec{u}) - p_{d+1-i}(\vec{x}) \bmod q.$$

Clearly the total degree of each p_j is (at most) j, and in particular the last polynomial $p_1(\vec{x})$ has degree (at most) 1, so there exists $\rho, \rho_0, \ldots, \rho_{n-1} \in \mathbb{Z}_q$ such that

$$p_1(\vec{x}) = \rho + \sum_{i=1}^{n-1} \rho_i \cdot x_i \bmod q. \tag{2}$$

Moreover, we can prove by induction on i that for every top-level encoding of zero v we have $|p_{d-i}(\vec{v}) \bmod q| < 2^i \cdot q^{3/4}$. This clearly holds for p_d, so now assume that it holds for p_{d+1-i} and we prove for p_{d-i}. Note that since both u, v are top-level encoding of zero then so is $v + u$, and therefore

$$
\begin{aligned}
|p_{d-i}(\vec{v})| &= |p_{d+1-i}(\vec{v} + \vec{u}) - p_{d+1-i}(\vec{v})| \\
&\leq |p_{d+1-i}(\vec{v} + \vec{u})| + |p_{d+1-i}(\vec{v})| < 2^{i-1}q^{3/4} + 2^{i-1}q^{3/4} = 2^i \cdot q^{3/4}.
\end{aligned}
$$

We conclude that for every top-level encoding of zero v we have $|\rho + \sum_{i=1}^{n-1} \rho_i \cdot v_i| < 2^{d-1} \cdot q^{3/4}$ (and note that since d is a constant then $2^{d-1} \cdot q^{3/4} \ll q$).

Step 2: Ignoring the Free Term

We note that the native GGH13 zero-test is linear whereas the polynomial p_1 is above is affine, so recovering a native GGH13 zero-test parameter seem to require that we ignore the free term. Indeed, below we show that the free term ρ from above must be small, and therefore we can ignore it without affecting the zero-test result.

To see that, note that by definition $\rho = p_1(\vec{0}) < 2^{d-1}q^{3/4}$, where the last inequality holds because in GGH13 the zero element is always a top-level encoding of zero. It follows that for every top-level encoding of zero $\vec{v}$ we have

$$|\sum_{i=1}^{n-1} \rho_i \cdot v_i| = |p_1(\vec{v}) - \rho| \leq |p_1(\vec{v})| + |\rho| < 2^d \cdot q^{3/4} \ll q. \tag{3}$$

Step 3: Recovering a Native GGH13 Zero-Test Parameter

Finally, we use the structure of the ring R_q to recover a native GGH13 zero-test parameter, i.e. a ring element $r \in R_q$ such that $\|r \cdot v \bmod q\| \ll q$ for every top-level encoding of zero v. Specifically we define $r(X) = \rho_0 - \sum_{i=1}^{n-1} \rho_{n-i} \cdot X^i \in R_q$, and we show that r is a native GGH13 zero-test parameter.

Let v be a top-level encoding of zero and denote $w = r \cdot v$. Since $R = \mathbb{Z}[x]/(x^n + 1)$, we have

$$\begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{n-1} \end{pmatrix} = \begin{pmatrix} \rho_0 & \rho_1 & \cdots & \rho_{n-2} & \rho_{n-1} \\ -\rho_{n-1} & \rho_0 & \cdots & \rho_{n-3} & \rho_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -\rho_2 & -\rho_3 & \cdots & \rho_0 & \rho_1 \\ -\rho_1 & -\rho_2 & \cdots & -\rho_{n-1} & \rho_0 \end{pmatrix} \cdot \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix}$$

Now by Eq. (3), we have

$$|w_0| = \left| \sum_{i=0}^{n-1} \rho_i \cdot v_i \right| < 2^d \cdot q^{3/4} \, .$$

Next, note that

$$\begin{pmatrix} -\rho_{n-1} & \rho_0 & \cdots & \rho_{n-3} & \rho_{n-2} \end{pmatrix} = \begin{pmatrix} \rho_0 & \rho_1 & \cdots & \rho_{n-2} & \rho_{n-1} \end{pmatrix} \cdot \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ -1 & & & \end{pmatrix} ,$$

and

$$\begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ -1 & & & \end{pmatrix} \cdot \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix} = \overrightarrow{-x^{n-1} \cdot v} \, .$$

Since $-x^{n-1} \cdot v$ is a valid top-level encoding of 0 when v is a top-level encoding of 0, we have that

$$|w_1| = \left| p'_{\vec{u}}(-x^{n-1} \cdot v) - \rho \right| < 2^d \cdot q^{3/4} \, ,$$

4

and similarly, for all $i = 2, \ldots, n-1$

$$|w_i| = \left| p'_{\vec{u}}(-x^{n-i} \cdot v) - \rho \right| < 2^d \cdot q^{3/4} \, .$$

Hence r is a native GGH13 zero-test parameter, and all zeroizing attacks on GGH13 apply directly to GHL.

Remark. Note that the argument above proves that $\|r \cdot v\| \ll q$ for all top-level encoding of zero, but it does not prove that $\|r \cdot v\| \approx q$ when v is a top-level encoding of a non-zero[2]; however, note that most zeroizing attacks do not require the latter equality to hold, but (essentially) only need r to be nonzero. Heuristically, however, it appears that this "should be the case", since $p_d(\vec{v}) \approx q$ whenever v is an encoding of a non-zero, and for $u \neq 0$ there is no reason to think that $p_d(\vec{v})$ and $p_d(\vec{u} + \vec{v})$ would be close to each other (and similarly for all the other p_{d-i}'s).

4 Conclusion

In this short note, we have shown that the Gentry-Halevi-Lepoint tentative fix of GGH13 does not thwart zeroizing attacks. Our attack is specific to GGH13, and is not applicable to CLT15 [CLT15], the tentative fix of CLT13 (also designed to have a "less-linear" zero-testing procedure).

References

[CGH+15] Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrède Lepoint, Hemanta K. Maji, Eric Miles, Mariana Raykova, Amit Sahai, and Mehdi Tibouchi. Zeroizing without low-level zeroes: New MMAP attacks and their limitations. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 247–266. Springer, August 2015.

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 3–12. Springer, April 2015.

[CLT13] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 476–493. Springer, August 2013.

[CLT15] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 267–286. Springer, August 2015.

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 1–17. Springer, May 2013.

[GGH+13b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th FOCS*, pages 40–49. IEEE Computer Society Press, October 2013.

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 498–527. Springer, March 2015.

[Hal15] Shai Halevi. The state of cryptographic multilinear maps, 2015. Invited Talk of CRYPTO 2015.

[HJ15] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH map. Cryptology ePrint Archive, Report 2015/301, 2015. http://eprint.iacr.org/2015/301.

---

[2]For example, it is easy to see that choosing the derivation point $u = 0$ would result in $r = 0$.