Zeroizing Without Low-Level Zeroes: New MMAP Attacks and their Limitations

Jean-Sébastien Coron[1], Craig Gentry[2], Shai Halevi[2], Tancrède Lepoint[3], Hemanta K. Maji[4,5], Eric Miles[4], Mariana Raykova[6(✉)], Amit Sahai[4], and Mehdi Tibouchi[7]

[1] University of Luxembourg, Luxembourg, Luxembourg
jean-sebastien.coron@uni.lu
[2] IBM Research, New York, USA
[3] CryptoExperts, Paris, France
tancrede.lepoint@cryptoexperts.com
[4] Center for Encrypted Functionalities, University of California, Los Angeles, USA
{enmiles,hmaji,sahai}@cs.ucla.edu
[5] Purdue University, West Lafayette, USA
[6] SRI International, Menlo Park, USA
mariana@cs.columbia.edu
[7] NTT Secure Platform Laboratories, Tokyo, Japan
tibouchi.mehdi@lab.ntt.co.jp

Abstract. We extend the recent zeroizing attacks of Cheon, Han, Lee, Ryu and Stehlé (Eurocrypt'15) on multilinear maps to settings where no encodings of zero below the maximal level are available. Some of the new attacks apply to the CLT13 scheme (resulting in a total break) while others apply to (a variant of) the GGH13 scheme (resulting in a weak-DL attack). We also note the limits of these zeroizing attacks.

Keywords: Cryptanalysis · Hardness assumptions · Multilinear maps

T. Lepoint—This work has been supported in part by the European Union's H2020 Programme under grant agreement number ICT-644209.

H. K. Maji, E. Miles and A. Sahai—Research supported in part from a DARPA/ONR PROCEED award, a DARPA/ARL SAFEWARE award, NSF Frontier Award 1413955, NSF grants 1228984, 1136174, 1118096, and 1065276, a Xerox Faculty Research Award, a Google Faculty Research Award, an equipment grant from Intel, and an Okawa Foundation Research Grant. This material is based upon work supported by the Defense Advanced Research Projects Agency through the U.S. Office of Naval Research under Contract N00014-11-1-0389. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense, the National Science Foundation, or the U.S. Government.

M. Raykova—This work has been supported in part from NSF Award 1421102.

R. Gennaro and M. Robshaw (Eds.): CRYPTO 2015, Part I, LNCS 9215, pp. 247–266, 2015.
DOI: 10.1007/978-3-662-47989-6_12

1 Introduction

The GGH13 [7] and CLT13 [6] "approximate multilinear maps" candidates suffer from *zeroizing attacks*, where encodings of zero at levels below the top (zero-test) level can be exploited to recover information that should have been hidden by the encoding scheme. The essence of these attacks is using successful zero tests to obtain equations over the base ring ($\mathbb{Z}$ or $\mathbb{Z}[X]/F(X)$), then solving these equations to get the desired information. First presented in the context of the GGH13 candidate [7], such attacks were recently extended by Cheon et al. [5] also to the CLT13 candidate, where they were shown to be particularly devastating, leading to a total break (when they can be mounted).

As explicitly discussed in [5], however, these attacks seem to depend on the availability of low-level encoding of zeros. This limits the applicability of these attacks, especially since several high-profile applications of multilinear maps (such as for obfuscation [8]) do not reveal such low-level zero encodings.

In this work we show that it is possible to "zeroize without low-level zeroes": that is, we extend the attacks from [5] and apply them against both CLT13 encodings and a matrix variant of GGH13 encodings, even in settings where no low-level encodings of zero are available to the adversary. We further systematize the new attacks and show that they can overcome recent proposals to "immunize" against them [3,9]. Our extensions to the attacks from [5] include replacing low-level zero encodings by "orthogonal encodings" (this extension was observed independently also by Boneh et al. [3]), dealing with cases where more than one monomial is needed to get a zero, and dealing with modifications of the CLT13 and GGH13 schemes that use matrix-based encodings with the encoded values embedded in the eigenvalues of the matrix. Before describing our zeroizing attacks, we discuss the impact and limitations of these attacks.

1.1 Impact of Our Attacks

Broken Assumptions and Constructions. The most direct consequence of our work is that more hardness assumptions and constructions from the literature are broken. Prior to our work, the attacks of [5] already broke several assumptions and constructions using CLT13 encodings because they provided low-level encodings of zero. Our work extends to new assumptions and constructions, even where no low-level encodings of zero are available. For example, our extensions can be used to break instances of the meta-assumption of Pass et al. [16] (using either GGH13 or CLT13 encodings), even when used without low-level encodings of zero. Furthermore, we show that natural attempts to "immunize" CLT13 or GGH13 encodings by removing low-level encodings of zero [3,9] fail. In particular, the assumptions used by Gentry et al. [10,11] are broken, even when "immunized" using the technique from [3]. Perhaps more surprisingly, we also show that simplified variants of certain obfuscation schemes can be broken:

- We show that the GGHRSW branching-program obfuscation procedure from [8], implemented over the CLT13 scheme [6], can be broken when it is applied to branching programs with a very specific "decomposable" structure. See Sect. 3.3.
- In the full version of this report, we also show that the simplified circuit obfuscation scheme of Zimmerman [17, Appendix A] and Applebaum-Brakerski [1] can be broken when applied to very simple circuits (e.g., point functions).

1.2 Limitations of Zeroizing Attacks

Potent as they are, zeroizing attacks have their limitations. For example, so far we do not have attacks on *any of the* NC^1 *obfuscation candidates in the literature*. Moreover the "dual-input straddling sets" technique that is used in several obfuscation schemes [2,4,17] appears to be effective in thwarting these attacks. See more details in Sect. 2.4.

Successful Zero Tests are Necessary. Our work demonstrate that some attacks are possible even if we only have top-level encoded zeros, but crucially all of these attacks depend on *successful zero tests* to get equations over the base ring. Some constructions or assumptions may not provide these zeros, and in that case it is plausible that the GGH13 and CLT13 candidates could even provide semantic security [12] of the encoded values. Even more, as far as we know the standard generic multilinear-map model could provide a good approximation of GGH13 and CLT13 in settings where top-level encoding of zeros are not available.

The Equations Must be Simple. In zeroizing attacks, each successful zero-test provides the adversary one equation over the base ring, and the attack relies on the attacker's ability to solve the resulting system of equations. The successful attacks detailed in our paper (as well as those from [5,7]) arise in situations where the adversary has *substantial freedom* in creating top-level encodings of zero, and can exploit this freedom to obtain "a simple system of equations" over the base ring that can be solved using linear algebraic techniques.

There are many cases, however, in which the available encodings are constructed such that only very particular combinations of them yield a top-level encoding of zero, and those combinations do not seem to yield efficiently solvable system of equations. Two such examples, illustrated in Sect. 2.4, are obfuscation schemes that rely on Barrington's theorem, and schemes that use the "dual-input straddling sets" technique.

We believe that long-term understanding of the security offered by current multilinear map candidates will require tackling long-standing questions about which kinds of systems of nonlinear equations are feasible to solve efficiently, and which are not.

2 Background and Overview

2.1 A Brief Description of the GGH13 and CLT13 Schemes

We begin with a brief description of the GGH13 and CLT13 schemes, omitting many details that are irrelevant for the attacks in question. Both these schemes implement graded encoding schemes where "plaintext elements" are encoded in a way that hides their value but allows to add and multiply them, and also allows to test if a degree-k expression in these values is equal to zero (where k is the "multi-linearity parameter").

The GGH13 Scheme. For GGH13 [7], the plaintext space is a quotient ring $R_g = R/gR$ where R is the ring of integers in a number field and $g \in R$ is a "small element" in that ring. The space of encodings is $R_q = R/qR$ where q is a "big integer". An instance of the scheme relies on two secret elements, the generator g itself and a uniformly random denominator $z \in R_q$. A plaintext element (which is a coset $a = \alpha + gR$) is encoded "at level one" as $u = [e/z]_q$ where e is a "small element" in the coset a (i.e., $e = \alpha + gr$ for some $r \in R$). More generally, a level-i encoding of the coset a has the form $u = [e/z^i]_q$ for a small $e \in \alpha + gR$.

Addition/subtraction of encodings at the same level is just addition in R_q, and it results in an encoding of the sum at the same level, so long as the numerators do not wrap around modulo q. Similarly multiplication of elements at levels i, i' is a multiplication in R_q, and as long as the numerators do not wrap around modulo q the result is an encoding of the product at level $i + i'$.

The scheme also includes a "zero-test parameter" in order to enable testing for zero at level k. Noting that a level-k encoding of zero is of the form $u = [gr/z^k]_q$, the zero-test parameter is an element of the form $\mathbf{p}_{\mathrm{zt}} = [hz^k/g]_q$ for a "somewhat small element" $h \in R$. This lets us eliminate the z^k in the denominator and the g in the numerator by computing $[\mathbf{p}_{\mathrm{zt}} \cdot u]_q = h \cdot r$, which is much smaller than q because both h, r are small. If u is an encoding of a non-zero α, however, then multiplying by $\mathbf{p}_{\mathrm{zt}}$ leaves a term of $[h\alpha/g]_q$ which is not small. Testing for zero therefore consists of multiplying by the zero-test parameter modulo q and checking if the result is much smaller than q.

Matrix-GGH13. An unpublished variant of GGH13 (that was meant to protect against zeroizing attacks) uses matrices of native GGH13 encodings, where the encoded value is an eigenvalue of the matrix and the zero-test parameter includes also the corresponding eigenvector. This is essentially the same as the GGHZ countermeasure construction from [9, Sect. 7] (which is described in Sect. 3.2), except that it uses GGH13 encodings rather than CLT13 encodings.[1]

[1] Our attack from Sect. 3.2 applies for the most part to this GGH13 variant too, except that in this case we only get a weak-DL attack rather than a complete break; see the full version for details.

The CLT13 Scheme. The CLT13 scheme [6] is similar to above, but it relies on CRT representation modulo a composite integer $x_0 = \prod_{j=1}^{n} p_j$, where the p_j's are "large primes", all of about the same size. We let $\mathsf{CRT}\,(a_1, \ldots, a_t)$ denote the unique element $a \in \mathbb{Z}_{x_0}$ that is congruent to a_j modulo p_j for all j. Also we often use the shorthand $\mathsf{CRT}\,(a_j)_j$ to denote the same.[2]

The plaintext space in CLT13 consists of vectors $\mathbf{a} \in \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$, where all the g_j's are much smaller than their corresponding p_j's. An instance of the scheme relies on the secrets g_j and p_j (with x_0 public), and on a secret uniformly random denominator $z \in \mathbb{Z}_{x_0}$. Such a vector $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$ is encoded at level one as $[\mathsf{CRT}\,(\alpha_1 + g_1 r_1, \ldots, \alpha_n + g_n r_n)\,/z]_{x_0}$, where the r_j's are all small. More generally a level-i encoding of this vector is of the form $[\mathsf{CRT}\,(\alpha_j + g_j r_j)_j\,/z^i]_{x_0}$.

Addition/subtraction of encodings at the same level is just addition in $\mathbb{Z}_{x_0}$, and it results in an encoding of the sum at the same level, so long as the numerators in the different CRT components do not wrap around modulo their respective p_j's. Similarly multiplication of elements at levels i, i' is a multiplication in $\mathbb{Z}_{x_0}$, and as long as the numerators in the different CRT components do not wrap around modulo their respective p_j's, the result is an encoding at level $i + i'$ of the entry- wise product of the two vectors.

For zero-testing, let us denote $p_j^* = x_0/p_j = \prod_{i \neq j} p_i$, and note the following easy corollary of the Chinese Remainder Theorem:

Proposition 1. *For all* $a_1, \ldots, a_n \in \mathbb{Z}$, $\mathsf{CRT}\left(p_j^* a_j\right)_j = \sum_{j=1}^{n} p_j^* a_j \pmod{x_0}$.

Namely when each CRT component j is divisible by p_j^*, then the CRT composition can be computed just by adding all the CRT components modulo x_0.

The zero-test parameter in CLT13 is $\mathbf{p}_{\mathrm{zt}} = [z^k \cdot \mathsf{CRT}\left(p_j^* h_j g_j^{-1}\right)_j]_{x_0}$ for small elements $h_j \ll p_j$, where g_j^{-1} is computed modulo p_j. Multiplying this zero-test parameter by a level-k encoding of zero, that has the form $u = [\mathsf{CRT}\,(g_j r_j)_j\,/z^k]_{x_0}$, yields

$$[\mathbf{p}_{\mathrm{zt}} \cdot u]_{x_0} = \mathsf{CRT}\left(p_j^* h_j r_j\right)_j = \sum_j p_j^* h_j r_j.$$

Since $h_j r_j \ll p_j$ for all j, then $p_j^* h_j r_j = (x_0/p_j) h_j r_j \ll x_0$, and also the sum is much smaller than x_0. Testing for zero therefore consists of multiplying by the zero-test parameter modulo x_0 and checking if the result is much smaller than x_0.

Common Properties. The GGH13 and CLT13 schemes share a very similar structure; here we summarize the common features that are used in the attacks:

- Each encoding is "associated" with the vector of small integers in the numerator. For GGH13 this is a 1-vector consisting of a single algebraic integer,[3]

[2] We do not assume that the a_j's are smaller than their corresponding p_j's.

[3] The matrix-GGH13 variant has vectors in the numerator rather than a single algebraic integer.

and for CLT13 this is a vector of n integers in $\mathbb{Z}$. Below we write informally $u \sim (a_1, \ldots, a_n)$ to denote the fact that the encoding u is associated with the vector of a_i's. Roughly speaking, the goal of the attacks is to recover the vector $(a_j)_j$ from the encoding u. Recovering this vector (even if not in full) is usually considered a break of the scheme.

- An encoding of zero is associated with a vector divisible by the g_j's, namely $u \sim (g_j r_j)_j$ for some r_j's.
- Addition and multiplication of encodings acts entry-wise on the vector of integers in the numerator. Importantly, the addition and multiplication of these vectors is done *over the integers, with no modular reduction.* This is because a wrap-around in these operations is an error condition, and so the parameters are always set to ensure that it does not happen.
- If $u \sim (g_j r_j)_j$ is an encoding of zero at the top level, then applying the zero-test to u returns the integer $w = \sum_j r_j \rho_j$, where the r_j's are the multipliers from the numerator vector and the ρ_j's are system parameters independent of u.

  In other words, applying the zero-test to an encoding of zero yields the inner-product of the associated vector (sans the g_j's) with a fixed secret vector. (In GGH13 this is the 1-vector (h), in CLT13 the vector is $(p_j^* h_j)_j$.) Importantly, here too the inner product is over the integers, with no modular reduction.

2.2 Overview of Existing Attacks

The GGH13 Zeroizing Attack. The following "zeroizing" attack on the GGH13 scheme was described in [7]. It gets as input a level-t encoding of zero $u_0 \sim (gr)$ and many other level-$(k-t)$ encodings $u_m \sim (a_m)$. Multiplying u_0 by any of the u_m's yields a top-level encoding of zero $u_0 u_m \sim (gra_m)$, and applying the zero-test yields the algebraic integer $w_m = hra_m$. Note that this almost recovers the numerators a_m's; indeed we have them up to the common factor $h' = hr$.

If we also knew the ideal $I_g = gR$ that defines the plaintext space, then being able to recover the numerator up to a constant is enough to break many hardness assumptions. For example, given an encoded matrix we could compute its determinant (mod I_g) up to a constant, which would tell us whether or not the encoded matrix has full rank.

Even when I_g is not explicitly given, Garg et al. described in [7] how it can be recovered in certain cases using GCD computations. Roughly, we can use GCD to identify and remove the common factor h', thereby getting the a_m's themselves, except that these are all algebraic integers so we only have GCD in terms of their ideals. Recovering the ideal $I_a = aR$ is not always useful, e.g., if I_a and I_g are co-prime then knowing I_a does not tell us anything about our plaintext coset $a + I_g$. However if some of the u_i's are themselves encoding of zero, namely $a_i = gr_i$, then given enough ideals $I_{a_i} = gr_i R$ we could again use GCD calculations to recover the ideal I_g itself, and then use that knowledge to attack the non-zero encodings among the u_i's. This attack was called in [7] a

"weak discrete-log attack". Recently, this attack was used by Hu and Jia [14] as a component in a new attack that breaks the key-exchange protocol from [7].

We note that the GGH13 zeroizing attack does not work against CLT13 encodings, since rather than a simple product we now have an inner product $w_m = \sum_j a_{m,j}\rho_j$, and we cannot use this to compute GCDs. (For the same reason, this attack does not work against the matrix-GGH13 variant.)

The CHLRS Zeroizing Attack. Cheon, Han, Lee, Ryu and Stehlé recently described in [5] a major upgrade of the GGH13 zeroizing attack, which can be used to completely break CLT13-based schemes in some cases, recovering the factorization of x_0 and all secret information. To mount the CHLRS zeroizing attack we need three sets of encoded inputs, which we denote by $\mathcal{A} = \{A_i : i = 1, \ldots, n\}$, $\mathcal{B} = \{B_0, B_1\}$, and $\mathcal{C} = \{C_j : j = 1, \ldots, n\}$ (with n the dimension of the numerator vectors). The A's are all random encoding of zeros, the B's are the target of the attack, and the C's are just helper encodings of random vectors. The levels of these encodings are such that multiplying $A_i \cdot B_\sigma \cdot C_j$ yields a top-level encoding of zero for any i, σ, j. Below we denote the numerator vectors associated with these encodings by

$$A_i \sim (g_1 r_{i,1}, \ldots, g_n r_{i,n}),\ B_\sigma \sim (b_{\sigma,1}, \ldots, b_{\sigma,n}),\ \text{and } C_j \sim (c_{j,1}, \ldots, c_{j,n}).$$

Multiplying $A_i \cdot B_\sigma \cdot C_j$ yields a top-level encoding of zero, associated with the vector $A_i \cdot B_\sigma \cdot C_j \sim (g_1 r_{i,1} b_{\sigma,1} c_{j,1}, \ldots, g_n r_{i,n} b_{\sigma,n} c_{j,n})$. Applying the zero-test we get a four-wise inner product, yielding the integer $w_\sigma[i,j] = \sum_{k=1}^{n} \rho_k r_{i,k} b_{\sigma,k} c_{j,k}$. We can write this four-wise inner product in matrix form as

$$w_\sigma[i,j] = (r_{i,1}\ \ldots\ r_{i,n}) \times \begin{pmatrix} \rho_1 b_{\sigma,1} & & \\ & \ddots & \\ & & \rho_n b_{\sigma,n} \end{pmatrix} \times \begin{bmatrix} c_{j,1} \\ \vdots \\ c_{j,n} \end{bmatrix},$$

and denote the vector on the left by $\mathbf{a}_i$, the matrix in the middle by B'_σ, and the vector on the right by $\mathbf{c}_j$. For a fixed σ, let i, j range over $1, \ldots, n$. This yields an $n \times n$ matrix of integers $W_\sigma = [w_\sigma[i,j]]_{i,j} = A' \times B'_\sigma \times C'$, where A' has the $\mathbf{a}_i$'s for rows and C' has the $\mathbf{c}_j$'s for columns. Since the $r_{i,k}$'s, $b_{\sigma,k}$'s, $c_{j,k}$'s and ρ_k's are all random (small) quantities, then with high probability the matrices are all invertible (over the rationals). Having computed the matrices W_σ, the attacker now sets

$$W = W_0 \times W_1^{-1} = (A' B'_0 C') \times (A' B'_1, C')^{-1} = A' \times (B'_0 \times {B'_1}^{-1}) \times {A'}^{-1}.$$

Observe now that $B^* = B'_0 \times {B'_1}^{-1}$ is a diagonal matrix with $b_{0,j}/b_{1,j}$ on the diagonal, and thus the eigenvalues of B^* are all the ratios $b_{0,j}/b_{1,j}$. And since W and B^* are similar matrices, then also the eigenvalues of W are the $b_{0,j}/b_{1,j}$'s. Hence once it computes W, the attacker can find its eigenvalues (over the rationals) and obtain all the ratios $b_{0,j}/b_{1,j}$.

These ratios may be enough by themselves to break some hardness assumptions, but for CLT13 it is possible to use them to factor x_0, thereby getting

a complete break. Specifically, since each ratio is rational it can be written as $u/v = b_{0,j}/b_{1,j}$ with u, v co-prime integers. Recalling now that B_0, B_1 are two encodings at the same level (say, level t) with numerator vectors $(b_{0,1}, \ldots, b_{0,n})$ and $(b_{1,1}, \ldots, b_{1,n})$, respectively, we get that

$$uB_1 - vB_0 = [\mathsf{CRT}\,(ub_{1,1} - vb_{0,1}, \ldots, ub_{1,n} - vb_{0,n})\,/z^t]_{x_0}.$$

This means that the j'th CRT component is $ub_{1,j} - vb_{0,j} = 0$, and with high probability the others are not, so we get $GCD(x_0, uB_1 - vB_0) = p_j$.

2.3 Extending the CHLRS Attack

In the current work we describe several extensions to attacks of Cheon et al. from [5]; below we describe these extensions briefly.

GGH13 vs. CLT13. We can also apply these zeroizing attacks to a matrix variant of GGH13, not just to CLT13 encodings, resulting in a "weak discrete-log" attack. This is described in the full version.

Orthogonal Encodings. We also note that these attacks do not actually require low-level encoding of zeros. Indeed all we need is that for every i, σ, j, the product $A_i B_\sigma C_j$ is a top-level encoding of zero, so we could have the A's with zeros in a few CRT components, the B's with zeros in some other components, and the C's with zeros in all the CRT components not covered by the A's and B's. This observation was also made concurrently by Boneh et al. [3].

More than One Monomial. The attack also extends to a setting where more than a single monomial is needed to get a zero. For example, consider the case where we have not three but six sets of encodings. Similar to before we have $\mathcal{A} = \{A_i : i = 1, \ldots, 2n\}$, $\mathcal{B} = \{B_0, B_1\}$, and $\mathcal{C} = \{C_j : j = 1, \ldots, 2n\}$, but now we also have $\tilde{\mathcal{A}} = \{\tilde{A}_i : i = 1, \ldots, 2n\}$, $\tilde{\mathcal{B}} = \{\tilde{B}_0, \tilde{B}_1\}$, and $\tilde{\mathcal{C}} = \{\tilde{C}_j : j = 1, \ldots, 2n\}$. (Note that the indices i, j now range over $[1, 2n]$, not $[1, n]$). The new attack requires that $A_i B_\sigma C_j + \tilde{A}_i \tilde{B}_\sigma \tilde{C}_j$ is a top-level encoding of zero for every i, σ, j. We denote the numerator vectors associated with these encodings by

$$A_i \sim (a_{i,1}, \ldots, a_{i,n}),\ \ B_\sigma \sim (b_{\sigma,1}, \ldots, b_{\sigma,n}),\ \ C_j \sim (c_{j,1}, \ldots, c_{j,n}),$$
$$\tilde{A}_i \sim (\tilde{a}_{i,1}, \ldots, \tilde{a}_{i,n}),\ \ \tilde{B}_\sigma \sim (\tilde{b}_{\sigma,1}, \ldots, \tilde{b}_{\sigma,n}),\ \ \tilde{C}_j \sim (\tilde{c}_{j,1}, \ldots, \tilde{c}_{j,n}).$$

We can think of the pairs $(A_i, \tilde{A}_i)$, $(B_\sigma, \tilde{B}_\sigma)$, $(C_j, \tilde{C}_j)$ as encodings that are associated with numerator vectors of twice the dimension, and the CHLRS attack can be applied to these new "double encodings". The only difference (other than the larger dimension) is that we can no longer associate the division-by-g_i with any single vector. Instead, applying the zero-test to $A_i B_\sigma C_j + \tilde{A}_i \tilde{B}_\sigma \tilde{C}_j$ yields a four-wise inner product *divided by the g_i's*, which we can write in matrix form:

$$w_\sigma[i,j] = (a_{i,1}\ \tilde{a}_{i,1}\ \ldots\ a_{i,n}\ \tilde{a}_{i,n}) \times \begin{pmatrix} \frac{\rho_1 b_{\sigma,1}}{g_1} & & & & \\ & \frac{\rho_1 \tilde{b}_{\sigma,1}}{g_1} & & & \\ & & \ddots & & \\ & & & \frac{\rho_n b_{\sigma,n}}{g_n} & \\ & & & & \frac{\rho_n \tilde{b}_{\sigma,n}}{g_n} \end{pmatrix} \times \begin{bmatrix} c_{j,1} \\ \tilde{c}_{j,1} \\ \vdots \\ c_{j,n} \\ \tilde{c}_{j,n} \end{bmatrix}.$$

Importantly, even though we have division by g_i's, this equation holds over the rationals, without modular reduction. The attack itself proceeds just as before, and the g_i^{-1} factors conveniently fall off when we compute $B'_0 \times {B'_1}^{-1}$. This extension can be used to break the "immunized" CLT13 variant from [3].

Using Cayley-Hamilton. In response to the CHLRS attacks, Garg et al. described in [9, Sect. 7] a variant of the CLT13 encoding that uses matrices for encoding, rather than single $\mathbb{Z}_{x_0}$ elements (see description in Sect. 3.2 below).

The attacks above apply also to this variant for the most part, but the resulting matrices B'_0, B'_1 are no longer diagonal. Instead they are block-diagonal with the block dimension corresponding to the dimension of the encoding matrices, and different blocks corresponding to different CRT components (i.e. $B_\sigma \bmod p_j$). The eigenvalues of $B'_0 \times {B'_1}^{-1}$ in this case need not be rational numbers anymore, they can be arbitrary complex numbers, and so the final step in the CHLRS attack cannot be applied.

However the characteristic polynomial of $B^* = B'_0 \times {B'_1}^{-1}$ is still the product of the characteristic polynomials of the blocks. We can factor the characteristic polynomial of B^* to find the block characteristic polynomials, and then apply these block polynomials to the matrix $M = B_1 \times B_0^{-1}$. Applying a block polynomial to M zeros out the corresponding CRT component (by the Cayley-Hamilton theorem), but not the others (whp), and we can then compute the GCD of x_0 and any matrix element to recover the prime corresponding to the zeroed CRT component. Note this assumes that the block polynomials are irreducible over $\mathbb{Q}$ (which indeed holds for [9, Sect. 7]), so that they can be efficiently found by factoring B^*'s characteristic polynomial.

The actual procedure that we use differs slightly, in order to handle an unpublished generalization of [9, Sect. 7] in which the encoding matrices themselves are constructed to be block-diagonal, say with block dimension d. With this change B^* is still block-diagonal, but the block dimension is now larger by a factor of d, and each polynomial that we want to apply to M is the product of d factors of B^*'s characteristic polynomial. We do not know of a way to efficiently partition these factors into the correct sets of size d. Instead, we remove one irreducible factor from B^*'s characteristic polynomial, and apply the resulting polynomial to M. This has the effect of zeroing out all CRT components *except* the one corresponding to the removed factor, so computing the GCD with x_0 recovers the product of all but one of the primes, and dividing x_0 by this recovers an individual prime. Cycling over all irreducible factors, we recover all of the primes.

2.4 Attack Limitations

As sketched in the introduction, zeroizing attacks have their limitations, in that they require zeros and moreover need the equations that yield these zeros to be "simple." Two scenarios that seem outside the scope of these attacks due to "non-simple" equations are discussed next.

Obfuscation Using Barrington's Theorem. Consider the obfuscation schemes in the literature that obfuscate matrix-based branching programs (BP) resulting from Barrington's theorem [2,4,8,16]. These schemes are designed so that the only way to get a top-level zero encoding is using the prescribed routines for evaluating the obfuscated circuit on various inputs, so we only need to examine the type of expressions that arise from such evaluation.

Recall that a matrix-based BP has a sequence of steps, each specified by two matrices and controlled by an input bit. On a given input, we choose one of the two matrices in each step (based on the corresponding input bit), then multiply all of the selected matrices in order to get the result. In the BPs that are generated by Barrington's theorem, each input bit controls several steps that are spaced far apart, and so changing the value of that bit changes the selection of all these matrices. This makes it hard to apply our attacks in this setting, since these attacks require a multilinear setting where we can get many different zeros by changing just a single variable in every monomial. Therefore, even though we do get equations over the base ring from top-level zeros in this scheme, these equations appear to be correlated in a highly non-linear manner, foiling our attempts to glean useful information from them.

We contrast this situation with the attack that we describe in Sect. 3.3, that breaks obfuscation of very simple branching programs which are "separable" in the sense that different subsets of the input bits control different consecutive intervals of steps, thus giving us the simple system of equations that we need.

Binding Variables. The CHLRS attacks and our extensions rely on the ability to partition the variables into groups ($\mathcal{A}, \mathcal{B}, \mathcal{C}$ above), so that we can independently choose variables from the different groups and every such choice yields a top-level zero. Several schemes in the literature use explicit binding variables to make it hard to partition the encodings into independent sets. For example, the obfuscation schemes of Barak et al. [2] and Zimmerman [17] use "dual-input straddling sets" to create a "high connectivity" interlocking set of encodings.

These schemes contain, for each pair i, j of input bits, four encoded variables $U_{i,j,0,0}, U_{i,j,0,1}, U_{i,j,1,0}$, and $U_{i,j,1,1}$, such that obtaining a top-level encoding of zero requires multiplying $U_{i,j,*,*}$'s that are consistent with some n-bit input x (i.e., it requires computing $\mathsf{some\ expression} \cdot \prod_{i,j} U_{i,j,x_i,x_j}$). This structure seems to foil attempts of separating the variables into independent sets, since changing any input bit creates a cascading effect. To illustrate the difficulty of applying the attack in this setting, we describe in the full version a relatively simple source-group hardness assumption involving such binding variables, which we do not know how to break even though we are given many low-level CLT13 encodings of zero.

3 A Unified Attack Against CLT13-Based Schemes

Below we present a general attack on CLT13-based schemes that combines all the ideas from Sect. 2.3, and show how this attack can be used against:

- The proposed CLT13 modification by Garg et al. [9, Sect. 7] (that was suggested in response to the CHLRS attacks);
- Obfuscations of branching programs with specific structure using the iO procedure of Garg et al. [8].

Central to our general attack is the notion of a "good attack set," which roughly plays the role of the sets $\mathcal{A}, \mathcal{B}, \mathcal{C}$ from Sect. 2 (together with the zero-test parameter). To define this notion formally, fix an instance of CLT13 with n secret primes $p_1, \ldots, p_n$ and modulus $x_0 := \prod_i p_i$. An *attack set* (of dimension d) consists of three sets of matrices $\mathcal{A}, \mathcal{B}, \mathcal{C} \subset \mathbb{Z}_{x_0}^{d \times d}$, of sizes $|\mathcal{A}| = |\mathcal{C}| = nd$ and $|\mathcal{B}| = 2$, and two vectors $s \in \mathbb{Z}_{x_0}^{1 \times d}$ and $t \in \mathbb{Z}_{x_0}^{d \times 1}$. These sets are constructed from the available public parameters and encodings of a given scheme, in such a way that for every choice of $(A_i, B_\sigma, C_j) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$, the value

$$W_\sigma[i,j] := s \times A_i \times B_\sigma \times C_j \times t \ \in \ \mathbb{Z}_{x_0}$$

is a zero-tested top-level encoding of 0. (The CHLRS attack can be thought as a special case where all the "matrices" are of dimension $d = 1$, and we have $s = 1$ and $t = \mathbf{p}_{\mathbf{zt}}$.) Given such an attack set, the attack proceeds as in Fig. 1, where we denote by $[z]_p$ the reduction of z modulo p into the interval $[-p/2, p/2)$, and this notation extends entry-wise to vectors and matrices.

Input: $\mathcal{A} = \{A_i\}_i,\ \mathcal{B} = \{B_\sigma\}_\sigma,\ \mathcal{C} = \{C_j\}_j,\ s,\ t$

1. Compute $(nd) \times (nd)$ matrices W_0, W_1 as $W_\sigma[i,j] := [s \times A_i \times B_\sigma \times C_j \times t]_{x_0}$.
2. Compute $W := W_0 \times W_1^{-1}$ over $\mathbb{Q}$, and $M := B_0 \times B_1^{-1} \pmod{x_0}$.
3. Compute W's characteristic polynomial $f := \mathsf{charPoly}(W)$ over $\mathbb{Q}$, and factor it into monic irreducible factors over $\mathbb{Q}$ as $f = f_1 f_2 \cdots f_m$.
4. For all $k \in \{1, \ldots, m\}$ define $F_k := f/f_k = \prod_{i \neq k} f_i \in \mathbb{Q}[X]$, let d_k be the common denominator of the coefficients of F_k, and set $G_k := F_k \cdot d_k$.
5. Evaluate the G_k's at the matrix M mod x_0, $M_k := [G_k(M)]_{x_0}\ \forall k \leqslant m$.
6. Compute $S := \{GCD(M_k[i,j], x_0) \mid i,j \in [nd]; k \in [m]\}$, and return $\{x_0/q \mid q \in S\}$.

Fig. 1. Our general attack on CLT13-based schemes

3.1 Sufficient Conditions for the Attack to Succeed

Next we state and prove sufficient conditions on the attack set that ensures that the attack in Fig. 1 succeeds. Specifically, we would like to show that each M_k in

step 5 must be zero modulo all the primes except one, and hence any non-zero entry in it yields a nontrivial factor of x_0 (i.e. the product of those primes).

Referring to the intuition from Sect. 2.3, the matrix $W = A \times B^* \times A^{-1}$ is similar to a block-diagonal matrix B^* that has one block for each CRT component. Specifically, the jth block of B^* is $B_j^* = [B_0]_{p_j} \times ([B_1]_{p_j})^{-1}$ (inverse over $\mathbb{Q}$). The characteristic polynomial of W is then the product of the characteristic polynomials of all the blocks. For simplicity, assume the block polynomials are the irreducible factors f_i from Fig. 1. Then each F_k is thus the product of all block polynomials except the kth, and by the Cayley-Hamilton theorem we have that $F_k(B_j^*) = 0$ (and therefore also $G_k(B_j^*) = 0$) for all blocks $j \neq k$. But $G_k(B_j^*) = 0$ over $\mathbb{Q}$ implies that also $G_k(B_0 \times B_1^{-1}) = 0 \pmod{p_j}$, so $G_k(M)$ is zero modulo all primes $j \neq k$. The only thing left to ensure is that for the last prime p_k we get $G_k(M) \neq 0 \pmod{p_k}$, which is the essence of our sufficient condition. The actual condition in Definition 1 below is slightly more complex, to account for the case when the block polynomials are reducible over $\mathbb{Q}$.

Definition 1. *Fix an attack set $(\mathcal{A}, \mathcal{B}, \mathcal{C}, s, t)$. Let B_0, B_1, M, W be the matrices from Fig. 1, and let $g_j := \mathsf{charPoly}\left([B_0]_{p_j} \times [B_1]_{p_j}^{-1}\right)$ over $\mathbb{Q}$. We say that $(\mathcal{A}, \mathcal{B}, \mathcal{C}, s, t)$ is* good *if:*

1. *$f := \mathsf{charPoly}(W) = \prod_{j \leqslant n} g_j$;*
2. *B_1 is non-singular modulo x_0;*
3. *The common denominators d_k from step 4 are all co-prime with x_0;*
4. *For any $j \leqslant n$ and any divisor f_k of g_j of degree $\geqslant 1$ (possibly $f_k = g_j$), denoting $G_k = d_k \cdot f/f_k$ as in step 4, we have $G_k(M) \neq 0 \pmod{p_j}$.*

Theorem 1. *For any good attack set $(\mathcal{A}, \mathcal{B}, \mathcal{C}, s, t)$, the algorithm in Fig. 1 recovers the secret primes $p_1, \ldots, p_n$.*

To prove Theorem 1 we use the following lemma:

Lemma 1. *Let $p > 1$ and $u_1, \ldots, u_t$, $v_1, \ldots, v_t$ be integers, s.t. the v_i's are invertible mod p, and denote $w_i = [u_i \cdot v_i^{-1}]_p$. If g is a multivariate integer polynomial such that $g(\frac{u_1}{v_1}, \ldots, \frac{u_t}{v_t}) = 0$ over $\mathbb{Q}$, then $g(w_1, \ldots, w_t) = 0 \pmod{p}$.*

Proof. It is enough to prove it for a linear g, since we can replace any non-linear term $\prod_{i \in I} (\frac{u_i}{v_i})^{e_i}$ (for some $I \subset [t]$ and e_i's) by new variables $u' = \prod_{i \in I} u_i^{e_i}$, $v' = \prod_{i \in I} v_i^{e_i}$, and $w' = [\prod_{i \in I} w_i^{e_i}]_p = [u' \cdot v'^{-1}]_p$, and then prove the same statement on the resulting new polynomial.

Now denote $V = \prod_i v_i$ and for each i denote $v_i^* = V/v_i = \prod_{j \neq i} v_j$. For a linear g we can write $\sum_i g_i \cdot \frac{u_i}{v_i} = 0$ over $\mathbb{Q}$, so also $\sum g_i u_i v_i^* = V \cdot \sum_i g_i \cdot \frac{u_i}{v_i} = 0$, and in particular $\sum g_i u_i v_i^* = 0 \pmod{p}$. Finally, since V is invertible modulo p we get

$$\sum_i g_i w_i = \sum_i g_i u_i v_i^{-1} = V^{-1} \cdot \sum_i g_i u_i v_i^* = 0 \pmod{p}. \qquad \square$$

Proof (of Theorem 1). For all i denote $B_i^* = [B_0]_{p_i} \times [B_1]_{p_i}^{-1}$ over $\mathbb{Q}$ and $\hat{B}_i = [B_0]_{p_i} \times [B_1]_{p_i}^{-1}$ over $\mathbb{Z}_{p_i}$. Let $t_i := det([B_1]_{p_i})$ (over $\mathbb{Q}$), and since B_1 is non-singular modulo x_0 then in particular $t_i \neq 0 \pmod{p_i}$. We can therefore write $B_i^* = \tilde{B}_i/t_i$ for an integer matrix $\tilde{B}_i$, and clearly we also have $\hat{B}_i = \tilde{B}_i \cdot t^{-1} \pmod{p_i}$.

Denote the characteristic polynomial of B_i^* over $\mathbb{Q}$ by $g_i := \mathsf{charPoly}(B_i^*)$. By the first condition in Definition 1 we have $f := \mathsf{charPoly}(W) = \prod_{j \leqslant n} g_j$. Note, however, that the g_j's are not necessarily irreducible, so there isn't necessarily a 1-1 correspondence between the g_j's and the irreducible factors f_k of f.

Fix an index $j \leqslant n$ and we show that for some k it holds that $G_k(M) \neq 0 \pmod{p_j}$ but $G_k(M) = 0 \pmod{p_i}$ for all $i \neq j$. Clearly this g_j is divisible by at least one f_k (which has degree $\geqslant 1$), so the last condition of Definition 1 implies that $G_k(M) = d_k \cdot F_k(M) \neq 0 \pmod{p_j}$. It remains to show that for all the other primes p_i, $i \neq j$, we have $G_k(M) = 0 \pmod{p_i}$.

Clearly F_k is divisible by g_i for every $i \neq j$, so the Cayley-Hamilton theorem implies that $F_k(B_i^*) = 0$ (over $\mathbb{Q}$) for all $i \neq j$, and therefore also $G_k(B_i^*) = 0$. Viewing $G_k(B_i^*)$ as a collection of multivariate polynomials over the elements of B_i^*, and using the facts that $B_i^* = \tilde{B}_i/t_i$ and $\hat{B}_i = \tilde{B}_i \cdot t^{-1} \pmod{p_i}$, we can apply Lemma 1 to conclude that also $G_k(\hat{B}_i) = 0 \pmod{p_i}$. And since $M = \hat{B}_i \pmod{p_i}$ then also $G_k(M) = 0 \pmod{p_i}$, as needed.

We have shown that $M_k := G_k(M)$ satisfies $M_k \neq 0 \pmod{p_j}$ but $M_k = 0 \pmod{p_i}$ for all $i \neq j$, so there exists an entry $z = M_k[a,b]$ such that $z \neq 0 \pmod{p_j}$ but $z = 0 \pmod{p_i}$ for all $i \neq j$. Thus $GCD(z, x_0) = \prod_{i \neq j} p_i$, and $x_0/GCD(z, x_0) = p_j$. □

Below we construct good attack sets for some schemes in the literature. More examples can be found in the full version. We will repeatedly use the fact that for a CLT13 encoding u associated with numerator vector $u \sim (r_i g_i + m_i)_i$, the randomization vector $(r_i)_{i \in [n]}$ is nearly uniform for each encoding. Specifically we have the following, which is proved in [3, Lemma 5.7].

Lemma 2 ([3]). *There exists a prime $q = 2^{\Omega(n)}$ which is determined by the CLT13 system parameters such that, for each encoding, the distribution on $(r_i \bmod q)_{i \in [n]}$ is $\mathsf{negl}(n)$-close to the uniform distribution on $\mathbb{Z}_q^n$.*

3.2 Attacking the Garg-Gentry-Halevi-Zhandry Countermeasure

Garg, Gentry, Halevi, and Zhandry proposed in [9, Sect. 7] a variant of the CLT13 scheme, that was designed to resist the CHLRS attack. This variant uses matrices of native CLT13 encodings, where the encoded value is an eigenvalue of the matrix and the zero-test parameter includes also the corresponding eigenvector. The CHLRS attack from [5] indeed does not apply to this variant, but below we show that this variant still gives rise to a good attack set, and thus our new attack from Fig. 1 recovers the secret primes.

The GGHZ variant relies on the same parameters as CLT13, namely we choose $(\{g_i\}_i, \{p_i\}_i, \mathbf{p}_{\mathrm{zt}}, \{z_i\})$ (with $x_0 := \prod_i p_i$ and top level corresponding to

denominator $z^* = \prod z_i$). Let $d := 2\kappa + 1$, and choose a secret matrix $T \in \mathbb{Z}_{x_0}^{d \times d}$ uniformly. An encoding of a plaintext value c at some level is given by $C \in \mathbb{Z}_{x_0}^{d \times d}$, where[4]

$$C := T \times \underbrace{\begin{bmatrix} \hat{\$} & \hat{0} & \dots & \hat{0} \\ \hat{0} & \hat{\$} & \dots & \hat{0} \\ \vdots & & & \vdots \\ \hat{0} & \hat{0} & \dots & \hat{c} \end{bmatrix}}_{C^*} \times T^{-1} \mod x_0.$$

Each $\hat{\$}$ in C^* is a "native CLT13 encoding" of an independent random value at the given level, each $\hat{0}$ is an independent native encoding of 0, and $\hat{c}$ is a native encoding of c. For zero-testing, two dimension-d vectors s, t are provided:

$$\begin{aligned} s &:= && [\hat{\$} \dots \hat{\$}\ \hat{0} \dots \hat{0}\ \hat{\$}] \times T^{-1} && \mod x_0 \\ t &:= \mathbf{p}_{\mathrm{zt}} \cdot T \times && [\hat{0} \dots \hat{0}\ \hat{\$} \dots \hat{\$}\ \hat{\$}]^T && \mod x_0 \end{aligned}$$

where $\hat{0}$ and $\hat{\$}$ are CLT13 native "level-zero" encodings (i.e., corresponding to denominator 1). Then a GGHZ-encoding C as above at the top level level can be zero tested by computing $s \times C \times t = (\hat{\$} \cdot \hat{c} + \hat{0}) \cdot \mathbf{p}_{\mathrm{zt}} \pmod{x_0}$ and checking for smallness.

Attack Set. The matrix sets $\mathcal{A}, \mathcal{B}, \mathcal{C}$ consist directly of GGHZ-encodings, since these are already in matrix form. Specifically, we assume that $[1, \kappa]$ is partitioned into three intervals $I_A = [1, k_A], I_B = [k_A + 1, k_B], I_C = [k_B + 1, \kappa]$, such that we have GGHZ-encodings

- $\mathcal{A} = \left\{ A_i = T \times A_i^* \times T^{-1} : A_i \text{ encoded at level } I_A \right\}_{i \in [nd]}$
- $\mathcal{B} = \left\{ B_\sigma = T \times B_\sigma^* \times T^{-1} : B_\sigma \text{ encoded at level } I_B \right\}_{\sigma \in \{0,1\}}$
- $\mathcal{C} = \left\{ C_k = T \times C_k^* \times T^{-1} : C_k \text{ encoded at level } I_C \right\}_{k \in [nd]}$

where $A_i \times B_\sigma \times C_k$ is a GGHZ-encoding of 0 for all $i, k \in [nd]$ and $\sigma \in \{0, 1\}$. The vectors s and t are the zero testing vectors from the GGHZ scheme.

Attack Set Properties. We prove that $(\mathcal{A}, \mathcal{B}, \mathcal{C}, s, t)$ form a good attack set according to Definition 1. We write

$$\begin{aligned} W_\sigma[i,k] &= s \times A_i \times B_\sigma \times C_k \times t \\ &= s \times T \times A_i^* \times B_\sigma^* \times C_k^* \times T^{-1} \times t \ = \ \mathbf{a}^i \times B_\sigma^* \times \mathbf{c}^k \end{aligned}$$

[4] The attack applies also when one uses many matrices $T_0, T_0^{-1}, \dots, T_\kappa, T_\kappa^{-1}$ (rather than just T, T^{-1}), so multiplication can only be performed in a specific order, as described in [9].

where $\mathbf{a}^i := s' \times A_i^*$ and $\mathbf{c}^k := C_k^* \times t'$ are dimension-d vectors. The above equality holds over the integers, not only modulo x_0, since all the variables in the final right-hand-side are small compared to x_0.

We denote $\mathbf{a}_\ell^i := \mathbf{a}^i \mod p_\ell$ and $\mathbf{c}_\ell^k := \mathbf{c}^k \mod p_\ell$ for $i \in [nd], \ell \in [n]$. Now we can write $W_\sigma = \tilde{A} \times \tilde{B}_\sigma \times \tilde{C}$, where $\tilde{A}$ is an $nd \times n^2 d$ matrix, $\tilde{C}$ is an $n^2 d \times nd$ matrix, and $\tilde{B}_\sigma$ is a $n^2 d \times n^2 d$ block-diagonal matrix, defined as follows.

$$\tilde{A} = \begin{bmatrix} \mathbf{a}_1^1 & \mathbf{a}_2^1 & \cdots & \mathbf{a}_n^1 \\ \mathbf{a}_1^2 & \mathbf{a}_2^2 & \cdots & \mathbf{a}_n^2 \\ \vdots & \vdots & & \vdots \\ \mathbf{a}_1^{nd} & \mathbf{a}_2^{nd} & \cdots & \mathbf{a}_n^{nd} \end{bmatrix} \quad \tilde{C} = \begin{bmatrix} (\mathbf{c}_1^1)^T & (\mathbf{c}_1^2)^T & \cdots & (\mathbf{c}_1^{nd})^T \\ (\mathbf{c}_2^1)^T & (\mathbf{c}_2^2)^T & \cdots & (\mathbf{c}_2^{nd})^T \\ \vdots & \vdots & & \vdots \\ (\mathbf{c}_n^1)^T & (\mathbf{c}_n^2)^T & \cdots & (\mathbf{c}_n^{nd})^T \end{bmatrix}$$

$$\tilde{B}_\sigma = \begin{bmatrix} B_\sigma^* \bmod p_1 & 0 & & 0 \\ 0 & B_\sigma^* \bmod p_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & B_\sigma^* \bmod p_n \end{bmatrix}$$

Using Lemma 2 and the Schwartz-Zippel lemma, it can be shown that with high probability over the randomness in the CLT13 encodings, $\tilde{A}$, $\tilde{C}$, and each B_σ^* have full rank nd. Under this condition each W_σ has rank nd and is thus invertible, so we can write $W = W_0 \times W_1^{-1} = \tilde{A} \times \tilde{B}_0 \times \tilde{B}_1^{-1} \times \tilde{A}^{-1}$, where $\tilde{A}^{-1}$ denotes the right inverse of the (non-square, full-rank) matrix $\tilde{A}$. Then we have

$$\begin{aligned} \mathsf{charPoly}(W) = \mathsf{charPoly}\left(\tilde{B}_0 \times \tilde{B}_1^{-1}\right) &= \prod_{i=1}^{n} \mathsf{charPoly}\left([B_0^*]_{p_i} \times [B_1^*]_{p_i}^{-1}\right) \\ &= \prod_{i=1}^{n} \mathsf{charPoly}\left([B_0]_{p_i} \times [B_1]_{p_i}^{-1}\right) \end{aligned}$$

so the first property of Definition 1 holds. The second property of Definition 1 holds with high probability over the choice of randomness in the CLT13 encodings. We were not able to prove that the last two properties in Definition 1 hold, but we verified them experimentally by running the attack on several random instances and checking that they indeed hold in all of them. For the fourth property, we can prove that it holds under the following natural conjecture:

Conjecture 1. For each $i \in [n]$, with high probability over the randomness in the CLT13 encodings, $\mathsf{charPoly}\left([B_0^*]_{p_i} \times [B_1^*]_{p_i}^{-1}\right)$ is irreducible over $\mathbb{Q}$.

We make two remarks about this conjecture. First, we have verified it experimentally. Second, a work of Kuba [15] shows that among the degree-n univariate integer polynomials whose coefficients are bounded in absolute value by an integer t, the polynomials that are reducible over $\mathbb{Q}$ make up a roughly $1/t$ fraction. In particular, a random polynomial with r-bit coefficients is irreducible over $\mathbb{Q}$ with probability roughly $1 - 2^{-r}$. Thus provided that $\mathsf{charPoly}\left([B_0^*]_{p_i} \times [B_1^*]_{p_i}^{-1}\right)$

is well-distributed among polynomials with an appropriate coefficient bound, Conjecture 1 should hold. We note that the relationship between a random polynomial and the characteristic polynomial of a random matrix has been explored by Hansen and Schmutz [13]. However, their results do not seem directly applicable here because they study polynomials over a finite field $\mathbb{F}$, and a uniform degree-n polynomial is irreducible over $\mathbb{F}$ only with probability $\approx 1/n$.

Assuming Conjecture 1, the fourth property of Definition 1 reduces to showing that for every prime factor p_j of x_0, $\left(\prod_{i\neq j} d_i f_i\right)(M) \neq 0 \pmod{p_j}$ where d_i, f_i, and M are as in Fig. 1. Choose all values in the CLT13 encodings except for the random values in the jth slot of the encodings in B_0, and call the unchosen values R. With high probability over this choice, each entry of M is a non-trivial linear polynomial in R, and $\left(\prod_{i\neq j} d_i f_i\right)$ is a non-trivial degree-$(n-1)$ polynomial in M. Thus each entry of $\left(\prod_{i\neq j} d_i f_i\right)(M)$ is a non-trivial degree-$(n-1)$ polynomial in R, and is non-zero modulo p_i with high probability by Lemma 2 and the Schwartz-Zippel lemma.

3.3 Attacking GGHRSW Obfuscation for Simple Branching Programs

We observe that our unified attack can be applied also to the candidate obfuscation construction of Garg et al. [8] when instantiated with the CLT13 multilinear maps and applied to branching programs with specific "partitionable" structure that we define below. We stress that applying Barrington's theorem to a circuits *does not have the required structure*, so as far as we know, the iO candidate from [8] for NC^1 circuits remains plausible.

The GGHRSW Obfuscation Candidate for Branching Programs. Recall that the obfuscator of Garg et al. [8] consists of encoded, randomized versions of two BPs; one is the BP that we want to obfuscate and the other is a "dummy BP" consisting of only identity matrices (and hence computing the all-one function). Even though neither program computes a zero, they are constructed such that their difference on accepting computations yields an encoding of zero, which can be recognized by zero testing. The core construction from [8] works with oblivious branching programs. An oblivious branching program of length L over ℓ input variables is defined as follows

$$BP = \{(\mathsf{inp}(i), A_{i,0}, A_{i,1}) : i \in [L], \mathsf{inp}(i) \in [\ell], A_{i,b} \in \{0,1\}^{w\times w}\},$$

where the $A_{i\sigma}$'s are invertible matrices and $\mathsf{inp}(i)$ is the input bit position examined in step i. The function computed by this branching program is defined (using some fixed matrix $A_0 \neq I$) as

$$f_{BP,A,I} = \begin{cases} 0 & \text{if } \prod_{i=1}^{L} A_{i,x_{\mathsf{inp}i}} = A_0 \\ 1 & \text{if } \prod_{i=1}^{L} A_{i,x_{\mathsf{inp}i}} = I \\ \mathsf{undef} & \text{otherwise.} \end{cases}$$

Let $\mathbb{Z}_p$ be a ring that we use for randomization, and for each input bit j denote by $I_j := \{i \in [L] : \mathsf{inp}(i) = j\}$ the set of steps where the branching program examine the j'th input bit. The GGHRSW construction, on input an L-step branching program BP over ℓ input bits, proceeds as follows:

1. Sample random and independent scalars $\{\alpha_{i,0}, \alpha_{i,1}, \alpha'_{i,0}, \alpha'_{i,1} \in \mathbb{Z}_p : i \in [L]\}$, subject to the constraint that for any input bit $j \in [\ell]$, we have $\prod_{i \in I_j} \alpha_{i,0} = \prod_{i \in I_j} \alpha'_{i,0}$ and $\prod_{i \in I_j} \alpha_{i,1} = \prod_{i \in I_j} \alpha'_{i,1}$.
2. Let $m = 2L + w$. For every $i \in [n]$, choose two block-diagonal $m \times m$ matrices $D_{i,0}, D_{i,1}$ where the diagonal entries $1, \ldots, 2L$ are chosen at random (\$) and the bottom-right $w \times w$ are the scaled $A_{j,b}$'s. Also choose two more $m \times m$ matrices $D'_{i,0}, D'_{i,1}$ where the diagonal entries $1, \ldots, 2L$ are random and the bottom-right $w \times w$ are the scaled identity:

$$D_{i,b} \sim \begin{pmatrix} \$ & & & \\ & \ddots & & \\ & & \$ & \\ & & & \alpha_{i,b} A_{i,b} \end{pmatrix}, \quad D'_{i,b} \sim \begin{pmatrix} \$ & & & \\ & \ddots & & \\ & & \$ & \\ & & & \alpha'_{i,b} I \end{pmatrix}, b \in \{0,1\}.$$

3. Choose vectors $\mathbf{s}$ and $\mathbf{t}$, and $\mathbf{s}'$ and $\mathbf{t}'$ of dimension $m = 2L + w$ as follows:

$$\begin{array}{ll} \mathbf{s} \sim & (0 \ldots 0 \ \$ \ldots \$ \quad \mathbf{s}^*) \\ \mathbf{s}' \sim & (0 \ldots 0 \ \$ \ldots \$ \quad \mathbf{s}'^*) \end{array} \qquad \begin{array}{ll} \mathbf{t} \sim & (\$ \ldots \$ \ \ 0 \ldots 0 \quad \mathbf{t}^*)^T \\ \mathbf{t}' \sim & (\$ \ldots \$ \ \ 0 \ldots 0 \quad \mathbf{t}'^*)^T \end{array}$$

   Here $\mathbf{s}^*, \mathbf{t}^*, \mathbf{s}'^*, \mathbf{t}'^* \in \mathbb{Z}_p^w$ are uniform up to $\langle \mathbf{s}^*, \mathbf{t}^* \rangle = \langle \mathbf{s}'^*, \mathbf{t}'^* \rangle$, and $0 \ldots 0$ and $\$ \ldots \$$ are length-L vectors of zeros and uniform elements of $\mathbb{Z}_p$, respectively.
4. Sample $2(L+1)$ uniform full-rank matrices $R_0, \ldots, R_L, R'_0, \ldots, R'_L \in \mathbb{Z}_p^{m \times m}$.
5. The randomized branching program over $\mathbb{Z}_p$ is the following:

$$\mathcal{RND}_p(BP) = \left\{ \begin{array}{ll} \tilde{\mathbf{s}} = \mathbf{s} R_0^{-1}, \ \tilde{\mathbf{t}} = R_n \mathbf{t}, & \tilde{\mathbf{s}}' = \mathbf{s}'(R'_0)^{-1}, \ \tilde{\mathbf{t}}' = R'_n \mathbf{t}' \\ \left\{ \tilde{D}_{i,b} = R_{i-1} D_{i,b} R_i^{-1} \right\}_{i \in [L], b \in \{0,1\}}, & \left\{ \tilde{D}'_{i,b} = R'_{i-1} D'_{i,b} (R'_i)^{-1} \right\}_{i \in [L], b \in \{0,1\}} \end{array} \right\}$$

6. Finally, encode the randomized program using an $(L+2)$-level asymmetric multilinear map scheme. Here we use the CLT13 scheme, choosing $x_0 = \prod_{i=1}^n p_i$, for equal-size primes p_i, $g = \mathsf{CRT}(g_i)$ for small $g_i \ll p_i$'s, random denominators $z_0, z_1, \ldots, z_{L+1} \in \mathbb{Z}_{x_0}$ with $z^* = [\prod_i z_i]_{x_0}$, and an element h with mid-size CRT components, used for the zero-testing parameter $\mathbf{p}_{\mathbf{zt}} = [h z^* g^{-1}]_{x_0}$.

   Choose random small vectors $\mathbf{r_s}$ $\mathbf{r'_s}$ $\mathbf{r_t}$ $\mathbf{r'_t}$, and random small matrices $U_{i,b}$ and $U'_{i,b}$, and publish the zero-testing parameter $\mathbf{p}_{\mathbf{zt}}$ and the obfuscation

$$\mathcal{O}(BP) \ = \ \left\{ \begin{array}{l} \hat{\mathbf{s}} = [z_0^{-1}(\tilde{\mathbf{s}} + g\mathbf{r_s})]_{x_0}, \qquad \hat{\mathbf{t}} = [z_{L+1}^{-1}(\tilde{\mathbf{t}} + g\mathbf{r_t})]_{x_0}, \\ \left\{ \hat{D}_{i,b} = [z_i^{-1}(\tilde{D}_{i,b} + gU_{i,b})]_{x_0} \right\}_{i \in [L], b \in \{0,1\}}, \\ \hat{\mathbf{s}}' = [z_0^{-1}(\tilde{\mathbf{s}}' + g\mathbf{r'_s})]_{x_0}, \qquad \hat{\mathbf{t}}' = [z_{L+1}^{-1}(\tilde{\mathbf{t}}' + g\mathbf{r'_t})]_{x_0}, \\ \left\{ \hat{D}'_{i,b} = [z_i^{-1}(\tilde{D}'_{i,b} + gU'_{i,b})]_{x_0} \right\}_{i \in [L], b \in \{0,1\}} \end{array} \right\}.$$

To evaluate $\mathcal{O}(BP)(x)$, compute $y = \tilde{s}\left(\prod_{i=1}^{L} \tilde{D}_{i,x_{\mathsf{inp}(i)}}\right)\tilde{t} - \tilde{s}'\left(\prod_{i=1}^{L} \tilde{D}'_{i,x_{\mathsf{inp}(i)}}\right)\tilde{t}'$, and output 1 if y encodes 0 (as determined by $\mathbf{p}_{\mathsf{zt}}$).

Attack. Our attack is applicable to branching programs with the following structure: there exists a partition of the input bits $[\ell] = X_1 \cup X_2 \cup X_3$ and the branching program steps $[L] = A \cup B \cup C$ such that A, B and C consist of consecutive steps in the branching program and $\mathsf{inp}(i) \in X_1\ \forall i \in A$, $\mathsf{inp}(i) \in X_2\ \forall i \in B$ and $\mathsf{inp}(i) \in X_3\ \forall i \in C$. We consider a branching program BP of length L and input length ℓ, computing the constant-1 function, that can be written as $BP(x) = A(x_1) \circ B(x_2) \circ C(x_3)$, where $A(x_1)$, $B(x_2)$, and $C(x_3)$ are branching programs over positions in the sets A, B, and C depending on inputs x_1, x_2, and x_3, respectively. We are given the obfuscation:

$$\mathcal{O}(BP) = \left(\mathbf{p}_{\mathsf{zt}}, \hat{\mathbf{s}}, \hat{\mathbf{t}}, \hat{\mathbf{s}}', \hat{\mathbf{t}}', \{\hat{D}_{i,b}, \hat{D}'_{i,b}\}_{i\in[L],b\in\{0,1\}}\right).$$

Attack Sets. We construct the sets $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ as follows. Let $A(x) = \prod_{i\in A} D_{i,x_{\mathsf{inp}(i)}}$, $A'(x) = \prod_{i\in A} D'_{i,x_{\mathsf{inp}(i)}}$. We define similarly $B(x), B'(x)$ and $C(x), C'(x)$. We note that using $\mathcal{O}$ we can compute $R_0 A(x) R_{|A|}^{-1} = \prod_{i\in A} \tilde{D}_{i,x_{\mathsf{inp}(i)}}$ and $R_0 A'(x) R_{|A|}^{-1} = \prod_{i\in A} \tilde{D}'_{i,x_{\mathsf{inp}(i)}}$, and so on. Let $\alpha_1, \ldots, \alpha_{mn} \in \{0,1\}^{|X_1|}$ be any set of distinct strings, and similarly for $\beta_0, \beta_1 \in \{0,1\}^{|X_2|}$ and $\gamma_1, \ldots, \gamma_{mn} \in \{0,1\}^{|X_3|}$. We set $s = (\tilde{s}, \tilde{s}')$ and $t = (\tilde{t}, -\tilde{t}')\mathbf{p}_{\mathsf{zt}}$, and define

$$\mathcal{A} = \left\{ \tilde{A}_i = \begin{bmatrix} R_0 A(\alpha_i) R_{|A|}^{-1} & 0 \\ 0 & R_0 A'(\alpha_i) R_{|A|}^{-1} \end{bmatrix} \right\}_{i\in[(2L+w)n]}$$

$$\mathcal{B} = \left\{ \tilde{B}_\sigma = \begin{bmatrix} R_{|A|} B(\beta_\sigma) R_{|A\cup B|}^{-1} & 0 \\ 0 & R_{|A|} B'(\beta_\sigma) R_{|A\cup B|}^{-1} \end{bmatrix} \right\}_{\sigma\in\{0,1\}}$$

$$\mathcal{C} = \left\{ \tilde{C}_k = \begin{bmatrix} R_{|A\cup B|} C(\gamma_k) R_L^{-1} & 0 \\ 0 & R_{|A\cup B|} C'(\gamma_k) R_L^{-1} \end{bmatrix} \right\}_{k\in[(2L+w)n]}.$$

Set Properties. We consider the values

$$W_0[i,k] = s \times \tilde{A}_i \times \tilde{B}_0 \times \tilde{C}_k \times t = (s \times A_i \times B_0 \times C_k \times t - s' \times A'_i \times B'_0 \times C'_k \times t')\mathbf{p}_{\mathsf{zt}}.$$

Since $W_0[i,k]$ is a zero-tested encoding of zero by the definition of the obfuscated branching programs, the above equality holds not only $\bmod x_0$ but also over the integers. W_1 is constructed analogously.

The rest of the attack proceeds in the same manner as the attack on GGHZ encodings from Sect. 3.2. Let $\mathbf{a}_i = (s \times A_i, s' \times A'_i)$ for $i \in [(2m+w)n]$, $\mathbf{c}_k = (C_k \times t \times \mathbf{p}_{\mathsf{zt}}, -C'_k \times t' \times \mathbf{p}_{\mathsf{zt}})$ for $k \in [(2m+w)n]$ and $X_0 = \begin{bmatrix} B_0 & 0 \\ 0 & B'_0 \end{bmatrix}$. We set the matrix $\hat{A}$ to have i-th row that is concatenations of the vectors $\mathbf{a}_i \bmod p_j$ for

$j \in [n]$, the matrix $\hat{C}$ to have i-th column that is concatenation of $\mathbf{c}_i^T \bmod p_j$ for $j \in [n]$, and the matrix $\hat{B}_0$ to be a diagonal matrix with diagonal consisting of $X_0 \bmod p_j$ for $j \in [n]$. Then we have that $W_0 = \hat{A} \times \hat{B}_0 \times \hat{C}$. We compute analogously $W_1 = \hat{A} \times \hat{B}_1 \times \hat{C}$. We use these matrices as in the attack on GGHZ encodings to break the underlying CLT13 encodings.

4 Conclusion

In this work we extended the recent CHLRS zeroizing attacks to many new settings, and also illustrated some of the limitations of this attack technique. The underlying message of recent attacks is that for current multilinear-map candidates, successful zero-tests give the adversary equations over the base ring (i.e. the integers or the ring of integers in a number field). Understanding the security of these candidates therefore hinges on a better understanding of which types of systems of nonlinear equations can be solved efficiently.

References

1. Applebaum, B., Brakerski, Z.: Obfuscating circuits via composite-order graded encoding. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part II. LNCS, vol. 9015, pp. 528–556. Springer, Heidelberg (2015). http://eprint.iacr.org/2015/025
2. Barak, B., Garg, S., Kalai, Y.T., Paneth, O., Sahai, A.: Protecting obfuscation against algebraic attacks. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 221–238. Springer, Heidelberg (2014). http://dx.doi.org/10.1007/978-3-642-55220-5_13
3. Boneh, D., Wu, D.J., Zimmerman, J.: Immunizing multilinear maps against zeroizing attacks. Cryptology ePrint Archive, Report 2014/930 (2014). http://eprint.iacr.org/
4. Brakerski, Z., Rothblum, G.N.: Virtual black-box obfuscation for all circuits via generic graded encoding. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 1–25. Springer, Heidelberg (2014)
5. Cheon, J.H., Han, K., Lee, C., Ryu, H., Stehlé, D.: Cryptanalysis of the multilinear map over the integers. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 3–12. Springer, Heidelberg (2015). http://eprint.iacr.org/2014/906
6. Coron, J.-S., Lepoint, T., Tibouchi, M.: Practical multilinear maps over the integers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 476–493. Springer, Heidelberg (2013). http://dx.doi.org/10.1007/978-3-642-40041-4_26
7. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (2013). http://dx.doi.org/10.1007/978-3-642-38348-9_1
8. Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: FOCS 2013, pp. 40–49. IEEE Computer Society (2013). http://doi.ieeecomputersociety.org/10.1109/FOCS.2013.13

9. Garg, S., Gentry, C., Halevi, S., Zhandry, M.: Fully secure functional encryption without obfuscation. Cryptology ePrint Archive, Report 2014/666 (2014). http://eprint.iacr.org/
10. Gentry, C., Lewko, A.B., Sahai, A., Waters, B.: Indistinguishability obfuscation from the multilinear subgroup elimination assumption. IACR Cryptology ePrint Archive 2014, 309 (2014). http://eprint.iacr.org/2014/309
11. Gentry, C., Lewko, A., Waters, B.: Witness encryption from instance independent assumptions. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 426–443. Springer, Heidelberg (2014). http://dx.doi.org/10.1007/978-3-662-44371-2_24
12. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. **28**(2), 270–299 (1984). http://dx.doi.org/10.1016/0022-0000(84)90070-9
13. Hansen, J.C., Schmutz, E.: How random is the characteristic polynomial of a random matrix? Math. Proc. Camb. Phi. Soc. **114**, 507–515 (1993)
14. Hu, Y., Jia, H.: Cryptanalysis of GGH map. Cryptology ePrint Archive, Report 2015/301 (2015). http://eprint.iacr.org/
15. Kuba, G.: On the distribution of reducible polynomials. Math. Slovaca **59**(3), 349–356 (2009)
16. Pass, R., Seth, K., Telang, S.: Indistinguishability obfuscation from semantically-secure multilinear encodings. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 500–517. Springer, Heidelberg (2014). http://dx.doi.org/10.1007/978-3-662-44371-2_28
17. Zimmerman, J.: How to obfuscate programs directly. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 439–467. Springer, Heidelberg (2015). http://eprint.iacr.org/2014/776