CONJURA · OPEN PROBLEM

Is XOR a Weak 2-Immunizer for Backdoored Generators?

Every other case in the source's table is settled; this one is left open, with a conjectured answer and a concrete route to it

Status. Statement: AI-written from Marshall Ball, Yevgeniy Dodis and Eli Goldin, *Immunizing Backdoored PRGs*, IACR ePrint 2023/1778. Not yet checked by a human. The source settles every other entry in its own table — XOR fails as a *strong* 2-immunizer under the Alekhnovich assumption, a bilinear pairing fails as a *weak* one under SXDH, a random oracle succeeds even with auxiliary input — and says of this one case that it leaves it open but conjectures it to be true.

Category. *Backdoored primitives; pseudorandom generators.*

Conjecture (informal). *A backdoored pseudorandom generator looks random to everyone except the saboteur who chose its public parameters. One defence is to run two of them and combine their outputs with a fixed function; if the result is secure whatever backdoors were planted, the function is an* immunizer. *XOR is the obvious candidate, and it demonstrably fails when both generators come from the same saboteur. The remaining case is the one where two* independent *designers — say two national standards bodies — each plant their own backdoor, and only afterwards pool what they know. The source conjectures XOR fails there too, and reduces the question to a concrete construction task: build two pseudorandom encryption schemes whose ciphertexts XOR to something jointly decryptable.*

1 The setting

A *backdoored PRG* is a pair (K, G) where K outputs a public parameter and a matching backdoor (pk, sk), and G_{pk} is a stateful generator: on state s it outputs a block and an updated state. Write $\mathrm{out}_q(G_{pk}, s)$ for the first q output blocks.

- (K, G) is (t, q, δ) *publicly secure* if $(pk, \mathrm{out}_q(G_{pk}, U_S))$ is δ-indistinguishable from (pk, U_{qn}) to distinguishers running in

time t — the public sees a good PRG.
- (K,G) is (t,q,δ) *backdoor secure* if the same holds when the distinguisher is also given sk.

An immunizer takes generators that are publicly secure but not backdoor secure and makes them backdoor secure. Given $C : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ and two generators, $C(G^X, G^Y)$ runs both independently and applies C blockwise to their outputs.

Definition 1 ([BDG23, Def. 2.8]). C is a (t,q,δ,δ')-*secure weak 2-immunizer* if for any two (t,q,δ) publicly secure PRGs (K^X,G^X) and (K^Y,G^Y), the PRG $((K^X,K^Y),C(G^X,G^Y))$ is (t,q,δ') backdoor secure.

Definition 2 ([BDG23, Def. 2.10]). C is a (t,q,δ,δ')-*secure strong 2-immunizer* if for any single (t,q,δ) publicly secure PRG (K,G), the PRG $(K,C(G,G))$ — two independent seeds, the *same* public parameter — is (t,q,δ') backdoor secure.

Strong implies weak, with a factor 4 loss in δ'. Weak is the setting where the two generators were designed by two independent key generation processes, with independent parameters and independent backdoors, and the two saboteurs join forces only at attack time.

2 Notation and parameters

- λ is the security parameter; t the distinguisher's running time, q the number of output blocks, δ and δ' the public and backdoor advantages.
- The parameter setting at issue throughout is $(\mathrm{poly}(\lambda),1,\mathrm{negl}(\lambda),\mathrm{negl}(\lambda)$ a single output block, negligible advantages, polynomial-time attackers.
- A public-key encryption scheme is *pseudorandom* if for every message the pair $(pk,\mathsf{Enc}_{pk}(m))$ is computationally indistinguishable from (pk,U) — strictly stronger than ordinary semantic security, and the notion the source uses throughout.
- Two schemes $(\mathsf{Gen},\mathsf{Enc},\mathsf{Dec})$ and $(\mathsf{Gen}',\mathsf{Enc}',\mathsf{Dec}')$ are *jointly* $\oplus$-*homomorphic* if there is a function $\mathsf{Dec}^{\oplus}_{sk,sk'}$ with $\Pr[\mathsf{Dec}^{\oplus}_{sk,sk'}(\mathsf{Enc}_{pk}(m;\alpha) \oplus \mathsf{Enc}'_{pk'}(m;\alpha')) = m] \geq 2/3$ for

every m, over the two key pairs and the two randomness strings.

3 The conjecture

Conjecture 1 ([BDG23, §1.3, §3.1]). *$\oplus$ is not a $(\mathrm{poly}(\lambda), 1, \mathrm{negl}(\lambda), \mathrm{negl}(\lambda))$-secure weak 2-immunizer.*

Remark 1 (How the source states it). The source states the direction, twice. Page 8, listing what its results do and do not settle: "The only exception is the explicit counter-example to the insecurity of XOR as a weak 2-immunizer, which we leave open (but conjecture to be true)." And page 13, immediately after proving the strong case: "Note that there is no simple way to adapt the public key encryption scheme used to prove this theorem to be sufficiently homomorphic to prove that XOR is not a weak 2-immunizer. We leave the question as to whether XOR is a weak 2-immunizer as an open question."

The parameter tuple in Conjecture 1 is the source's own, carried over from the theorem it is the missing counterpart to (Theorem 2), and the source's Corollary 3.13 states the sufficient condition at exactly these parameters.

Theorem 1 (The route the source names, [BDG23, Cor. 3.13]). *If there exist $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ and $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ that are pseudorandom and jointly $\oplus$-homomorphic, then $\oplus$ is not a $(\mathrm{poly}(\lambda), 1, \mathrm{negl}(\lambda), \mathrm{negl}(\lambda))$-secure weak 2-immunizer.*

This is a sufficient condition, not a characterisation: nothing in the source says a counterexample must arise this way. But it is the source's own suggested route, and it comes with a stated expectation: "We remark that the Alekhnovich PKE is not jointly $\oplus$-homomorphic with itself. We leave it as an open question as to whether such a pair of encryption schemes exist for XOR, but we suspect that its existence is likely."

Remark 2 (Why the strong case does not settle the weak one).

Theorem 2 ([BDG23, Thm. 3.1]). *Assuming the Alekhnovich assumption, $\oplus$ is not a $(\mathrm{poly}(\lambda), 1, \mathrm{negl}(\lambda), \mathrm{negl}(\lambda))$-secure* strong *2-immunizer.*

The implication between the two notions runs the wrong way. Strong security implies weak security, so a counterexample to strong security says nothing about weak security — and the counterexample is exactly where the two settings come apart. To break the strong notion one needs a single pseudorandom scheme that is $\oplus$-homomorphic *with itself*: two ciphertexts under the *same* public key whose XOR decrypts. Alekhnovich's LPN-based encryption is, which is what Theorem 2 uses. To break the weak notion one needs two schemes with *independent* keys whose ciphertexts of the same message XOR to something decodable from both secret keys, and the source states plainly that Alekhnovich's scheme is not jointly $\oplus$-homomorphic with itself.

Remark 3 (The evidence on each side). For the conjecture. Every other case the source examines resolves against the simple candidates, including one in the weak setting: a bilinear pairing $e : \mathbb{G}_X \times \mathbb{G}_Y \to \mathbb{G}_T$ — which, as an operation on two independently keyed sources, "looks similar to XOR" — is not a secure weak 2-immunizer under SXDH. That is a worked instance of the very shape Theorem 1 asks for, built by constructing schemes jointly homomorphic under a related operation.

Against it, or at least in the way. The source's black-box separation says no 2-immunizer that is "highly dependent on both inputs" — XOR included — can be *proved* secure by reduction to an efficiently falsifiable assumption. That rules out one kind of positive answer but not the positive answer itself: XOR could still be a weak 2-immunizer with no such proof available. So Conjecture 1 does not follow from the separation, and this is the gap the source is pointing at.

Remark 4 (What a resolution looks like). A refutation of Conjecture 1 — a proof that XOR *is* a weak 2-immunizer — would, by the separation just described, have to be non-black-box or rest on a non-falsifiable assumption, and would be the more surprising outcome.

A proof of it is a construction: two pseudorandom public-key encryption schemes, jointly $\oplus$-homomorphic, under any assumption at all. The source's expectation is that these exist, and the honest reading of the open problem is that nobody has yet written one down rather than that anything is known to block it.

Remark 5 (The separate question the source calls fascinating). Not published here, and not to be confused with Conjecture 1: "Is there a 2-immunizer C in the standard model whose security can be black-box reduced to an efficiently falsifiable assumption?" The source's separation shows such a C cannot be highly dependent on both inputs, which excludes every natural candidate including cryptographic hash functions, and the source names two possible ways round — a non-black-box reduction from a function like a strong two-source extractor, or a non-falsifiable assumption in the style of universal computational extractors. That is a different statement, posed separately by the source.

4 Bibliography

[BDG23] Marshall Ball, Yevgeniy Dodis and Eli Goldin. *Immunizing backdoored PRGs.* IACR ePrint 2023/1778. The source. The conjecture is stated on page 8 and again on page 13; the definitions of weak and strong 2-immunizer are Definitions 2.8 and 2.10; joint $\oplus$-homomorphism is Definition 3.11 with Theorem 3.12 and Corollary 3.13 on page 17; the strong-case counterexample is Theorem 3.1; the pairing counterexample is Theorem 3.3; the black-box separation is Theorem 1.4; the random-oracle positive result is Theorem 1.3.

[DGGJR15] Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels and Thomas Ristenpart. *A formal treatment of backdoored pseudorandom generators.* EUROCRYPT 2015, Part I, LNCS 9056, pages 101–126, Springer, April 2015. The work the source continues: it initiated the question of immunizing backdoored PRGs, and its seeded 1-immunizers are built from universal computational extractors.

[Ale11] Michael Alekhnovich. *More on average case vs approximation complexity.* Computational Complexity, 20(4):755–786, December 2011. The LPN-style public-key encryption scheme that is $\oplus$-homomorphic with itself, and so refutes XOR as a strong 2-immunizer — but is not jointly $\oplus$-homomorphic with itself, which is why the weak case stays open.