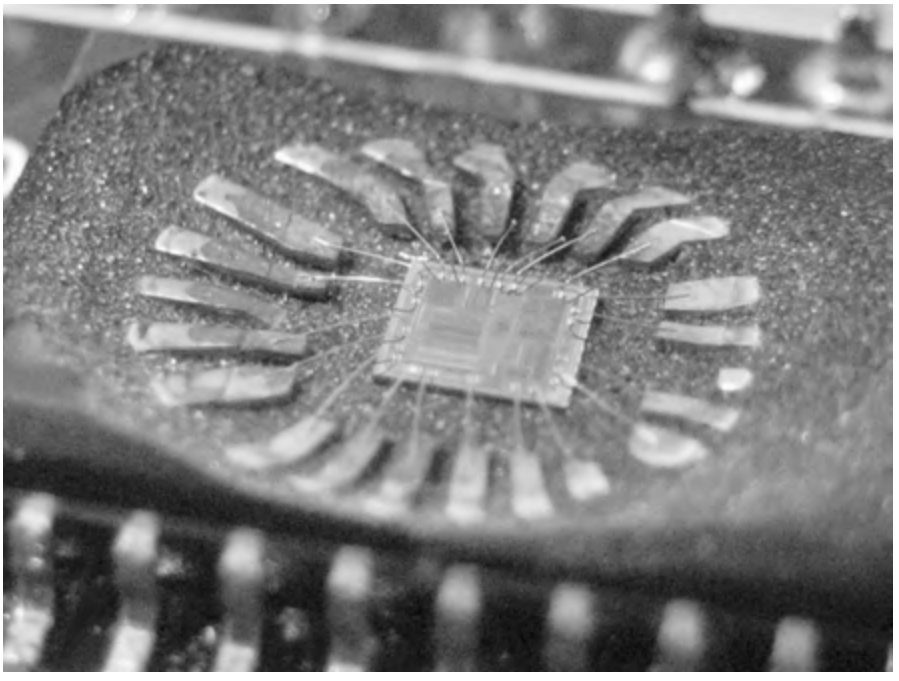
Dekapsulacja, usuwanie warstw ochronnych i ponowne łączenie

Dekapsulacja to proces usuwania części materiału z obudowy układu scalonego za pomocą środków chemicznych, zwykle przez wkraplanie oparów kwasu azotowego lub siarkowego na obudowę chipa, aż się ona rozpuści. Rezultatem jest dziura w obudowie, przez którą można zbadać sam mikrochip. Jeśli zostanie to zrobione poprawnie, to chip nadal będzie działał.

UWAGA *Dekapsulację można przeprowadzić w domu, o ile na miejscu dysponujemy wyciągiem laboratoryjnym i innymi zabezpieczeniami. Dla odważnych: szczegółowe informacje o tym, jak przeprowadzić dekapsulację w warunkach domowych, zawiera biblia* PoC||GTFO *wydana przez No Starch Press.*

Podczas *usuwania warstw ochronnych* (ang. *depackaging*) obudowę zanurza się w kwasie, po czym w rezultacie dostępne jest wnętrze chipa. Aby przywrócić jego funkcjonalność, należy ponownie połączyć chip, co oznacza ponowne podłączenie maleńkich wyprowadzeń, które normalnie łączą go z pinami w obudowie (patrz rysunek 1.8).



Rysunek 1.8. Odsłonięty chip wraz z jego widocznymi drucikami połączeniowymi (Travis Goodspeed, licencja CC BY 2.0)

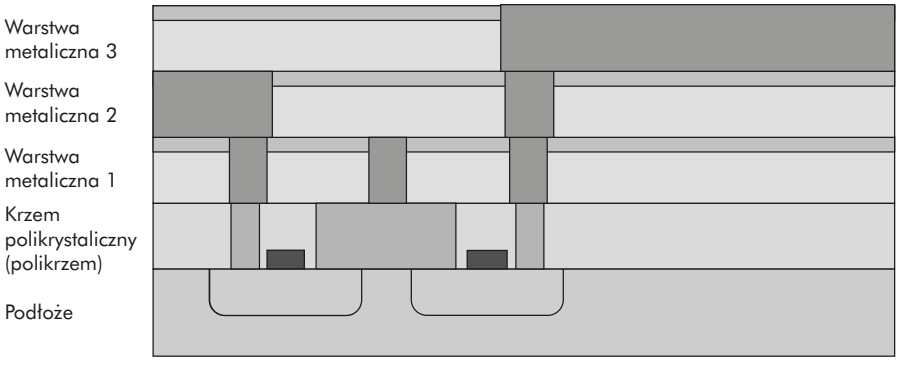
Mimo że mogą one paść w trakcie tego procesu, uszkodzone chipy nadają się do tworzenia obrazów i optycznej inżynierii odwrotnej. Jednak w wypadku większości ataków chipy muszą być sprawne.

Obrazowanie mikroskopowe i inżynieria wsteczna

Po odsłonięciu wnętrza chipa pierwszym krokiem jest identyfikacja jego większych bloków funkcjonalnych, a konkretnie – znalezienie interesujących bloków. Rysunek 1.2 pokazuje niektóre z tych struktur. Największymi blokami na matrycy będzie pamięć, taka jak statyczna pamięć RAM (SRAM) dla pamięci podręcznej procesora lub pamięć TCM (ang. *tightly coupled memory*), oraz ROM dla kodu rozruchu. Wszelkie długie, w większości proste wiązki linii to magistrale łączące procesory i urządzenia peryferyjne. Znajomość względnych rozmiarów i tego, jak wyglądają poszczególne struktury, pozwala rozpocząć inżynierię odwrotną chipów.

Gdy odsłonięte jest wnętrze chipa, jak na rysunku 1.8, widać tylko górną warstwę metaliczną. Aby wykonać inżynierię wsteczną całego chipa, musimy go *podzielić na warstwy*, co oznacza zdjęcie poszczególnych metalicznych warstw chipa, aby odsłonić kolejne, znajdujące się pod nim.

Rysunek 1.9 przedstawia przekrój układu scalonego w technologii CMOS (ang. *complementary metal oxide semiconductor*), która jest sposobem budowy większości współczesnych układów. Jak widać, tranzystory (krzem polikrystaliczny / podłoże) łączy wiele warstw i przelotek z metali zawierających miedź. Warstwa metaliczna najniższego poziomu służy do tworzenia *standardowych komórek*, które są elementami tworzącymi bramki logiczne (AND, XOR itd.) z wielu tranzystorów. Warstwy metaliczne najwyższego poziomu są zwykle używane do zarządzania zasilaniem i zegarem.



Rysunek 1.9. Przekrój układu scalonego w technologii CMOS