Teil I: Kurzbericht

In VE-CirroStrato mussten RFET-basierte Tarnschaltungen entwickelt und demonstriert werden, die die Funktionalität klassischer Tarn- und Logikverriegelungsansätze effektiv kombinieren. RFET-basierte Konzepte sind unabhängig vom zugrundeliegenden Design und können verwendet werden, um jede digitale Schaltung vor IP-Diebstahl zu schützen. IP-Schutzschaltungen aus RFETs übertreffen damit die Fähigkeiten CMOS-basierter Systeme, bei denen die elektrischen Bauteileigenschaften zur eindeutigen Identifizierung verwendet werden können. Um die optimale Funktionalität der Schutzschaltungen zu gewährleisten, muss bei der Logiksynthese die gezielte Platzierung der RFET-Gates berücksichtigt werden. Der gezielte Einbau von Zellen sollte einerseits die Schutzwirkung maximieren und andererseits den Mehraufwand hinsichtlich Fläche, Signallaufzeit und Stromverbrauch so gering wie möglich halten. Insgesamt war ein deutlich reduzierter Aufwand zu erwarten als bei vergleichbaren CMOS-basierten Schutzschaltungen.

Um das Gesamtziel zu erreichen, waren folgende konkrete Arbeitsziele vorgesehen:

- Entwurf sicherer digitaler Schaltungsblöcke auf Basis von RFETs als Zusatztechnologie für 22 nm FDSOI und Entwicklung einer umfassenden Bibliothek (Library Blocks) daraus.

- Entwicklung einer automatisierten Designumgebung (EDA), um die logische und physikalische Synthese sicherer Schaltungen auf Basis von RFETs integriert in einen 22 nm FDSOI Tool Flow zu ermöglichen.

- Entwurf von Algorithmen, die RFET-Zellen automatisch in beliebige integrierte Schaltungen platzieren. Dadurch soll einerseits der Schutzgrad maximiert und andererseits der Mehraufwand an Fläche, Energie und Signallaufzeiten minimiert werden.

Die Arbeiten waren in mehreren Arbeitspaketen geplant, die von Zelldesign und -modellierung über Integration und Charakterisierung bis hin zu Verifizierung und Test reichten. Der letzte Teil wurde in Zusammenarbeit mit der Bremer Gruppe durchgeführt.

Unsere Arbeit kann in zwei Teile unterteilt werden. Der erste Teil betrifft HW-Sicherheitsverfahren, die die Eigenschaften von RFET-Bauteilen ausnutzen können. Zu diesem Zweck haben wir verschiedene IP-Schutzverfahren untersucht, insbesondere Camouflaging und Logic Locking. Wir zeigen, dass die RFET-Eigenschaften genutzt werden können, um sehr kompakte sichere Zellen mit akzeptabler Leistung für diese Verfahren

zu entwickeln. Wir stellen ein Tool zur Verfügung, mit dem Camouflaging und Logic Locking in den Synthesefluss integriert werden können, basierend auf den Anforderungen des Hardware-Sicherheitsdesigners. Darüber hinaus entwerfen wir einen algorithmischen Fluss, der darauf abzielt, sichere RFET-Zellen für Logic Locking und Layout Camouflaging zu nutzen, um die Sicherheit bei akzeptablem Overhead zu maximieren.

Der zweite Teil zielt darauf ab, einen EDA-Flow für den RFET-basierten Schaltungsentwurf bereitzustellen. Die Grundvoraussetzung für die RFET-basierte Synthese ist eine Technologiebibliothek mit Standardzellen namens Liberty. Wir bieten einen automatischen Ablauf zur Erzeugung der RFET-basierten Liberty-Datei unter Verwendung eines kommerziellen Charakterisierungswerkzeugs. Außerdem erstellen wir eine LEF-Datei für RFET-basierte Logikzellen, um den gesamten EDA-Flow für RFET-basiertes ASIC-Design bereitzustellen.

Verbundprojekt: „Neuartige rekonfigurierbare Transistoren für den Knowhow-Schutz von Elektronikkomponenten – VE-CirroStrato“

CIRROSTRATO

Teilvorhaben: „Synthese- und Layoutwerkzeuge für Knowhow-Schutzkonzepte auf Basis neuartiger rekonfigurierbarer Transistoren“

Abschlussbericht: 01.03.2021 – 31.08.2024

Schlussbericht Teil II

1. Zusammenfassung
2. Soll-Ist-Vergleich, Meilensteine
3. Detaillierten Ergebnissen
4. Zusätzliche Informationen

1. Zusammenfassung

Unsere Arbeit kann in zwei Teile unterteilt werden. Der erste Teil betrifft HW-Sicherheitsverfahren, die die Eigenschaften von RFET-Bauteilen ausnutzen können. Zu diesem Zweck haben wir verschiedene IP-Schutzverfahren untersucht, insbesondere Camouflaging und Logic Locking. Wir zeigen, dass die RFET-Eigenschaften genutzt werden können, um sehr kompakte sichere Zellen mit akzeptabler Leistung für diese Verfahren zu entwickeln. Wir stellen ein Tool zur Verfügung, mit dem Camouflaging und Logic Locking in den Synthesefluss integriert werden können, basierend auf den Anforderungen des Hardware-Sicherheitsdesigners. Darüber hinaus entwerfen wir einen algorithmischen Fluss, der darauf abzielt, sichere RFET-Zellen für Logic Locking und Layout Camouflaging zu nutzen, um die Sicherheit bei akzeptablem Overhead zu maximieren.

Der zweite Teil zielt darauf ab, einen EDA-Flow für den RFET-basierten Schaltungsentwurf bereitzustellen. Die Grundvoraussetzung für die RFET-basierte Synthese ist eine Technologiebibliothek mit Standardzellen namens Liberty. Wir bieten einen automatischen Ablauf zur Erzeugung der RFET-basierten Liberty-Datei unter Verwendung eines kommerziellen Charakterisierungswerkzeugs. Außerdem erstellen wir eine LEF-Datei für RFET-basierte Logikzellen, um den gesamten EDA-Flow für RFET-basiertes ASIC-Design bereitzustellen.

Nachfolgend erläutern wir die durchgeführten Teilprojekte im Vergleich zum ursprünglich geplanten Zeitplan.

2. Soll-Ist-Vergleich, Meilensteine

Tabelle 1: Arbeitspakete „Ist und „Soll“ mit TU Dresden-Anteil

Lfd. Nr.	Meilensteine der Arbeitspakete	Zeitplan „Soll“	Zeitplan „Ist“	AP abgeschlossen/ MS erfüllt
MSZ	Zentraler Meilenstein zum Projekt-Monitoring	**10/2022**	**10/2022**	**erfüllt**
AP 1	**Zellendesign und Modellierung**		**8/2022**	
1.1	Konzeption zur Anwendung von RFETs für den IP-Schutz	2/2022	2/2022	abgeschlossen
1.5a	SPICE Simulationen der Zellen für Sicherheitsgrundschaltungen	8/2023	12/2023	abgeschlossen
1.5b	Konvertierung in Liberty-Modelle für RFET/CMOS Co-Design	8/2023	6/2024	abgeschlossen

AP 2	**Integration und Charakterisierung**	**11/2023**	**8/2024**	
2.1a	Erstellung von Gen-lib Bibliotheken als Basis für Entwurf für einen RFET kompatiblen EDA Toolfluss	8/2022	8/2022	abge-schlossen
2.1b	Erstellung von LEF-Bibliotheken als Basis für Layout für einen RFET kompatiblen EDA Tool-fluss	8/2022	6/2024	abge-schlossen
2.2a	Basissetup für Logische Synthese und Erstel-lung von Netzlisten	2/2023	12/2022	abge-schlossen
2.2b	Einbindung der Konzepte zum IP-Schutz in der logischen Synthese	2/2023	12/2022	abge-schlossen
2.3a	Algorithmen zur Platzierung von RFET Zellen hinsichtlich Maximierung der Sicherheit	8/2023	7/2024	abge-schlossen
2.3b	Algorithmen zur Platzierung von RFET Zellen hinsichtlich Minimierung des Overheads	8/2023	7/2024	abge-schlossen
2.4a	Basissetup für Physikalischer Synthese	8/2023	12/2023	abge-schlossen
2.4b	Physikalische Synthese von RFET-Sicherheits-zellen in RFET/CMOS Co-Design	8/2023	8/2024	abge-schlossen
2.5a	Place, Route eines virtuellen Schaltungsde-monstrators	2/2024	8/2024	abge-schlossen
2.5b	Integration der EDA Umgebung in 22 nm FDSOI Standard Toolfluss	2/2024	8/2024	abge-schlossen
MS5	Gen-lib Bibliothek für Entwurf von RFET Schaltungen entwickelt.	**8/2022**	**8/2022**	**erfüllt**
MS9	EDA Werkzeuge für logische und physikali-sche Synthese von RFET/CMOS Ko-Design und Algorithmen.	**02/2024**	**02/2024**	**erfüllt**

AP 4	**Verifikation and Test**	**02/2024**	**02/2024**	
4.5	Vergleich mit CMOS Schutzschaltungen hin-sichtlich Sicherheit, Fläche, Leistung und Ener-gieverbrauch	02/2024	8/2024	abge-schlossen
4.6	Verwertungserkundung, Zertifizierungskonzept	11/2023	8/2024	abge-schlossen
MS10	Benchmark mit CMOS-Lösungen anhand eines virtuellen Demonstrators; Verwertungs- und Zertifizierungskonzept	**02/2024**	**02/2024**	**erfüllt**

3. Detaillierten Ergebnissen

Dieser Abschnitt wird auf Englisch präsentiert, da die wichtigsten Ergebnisse in dieser Sprache veröffentlicht wurden.

Detailed presentation of the results

Work Package WP 1: Cell Design and Modelling

Task 1.5a: Spice simulations of the cells for basic safety circuits

a) Goal

Spice simulation of the RFET-based secure cells to extract timing and power features.

b) Current States and Results

In our previous steps, we prepared a circuit-level simulation environment to extract the timing and power information of basic RFET cells (INV, NAND, NOR), reconfigurable logic cells (MIN/NAND/NOR and XOR/XNOR), and larger circuits like multipliers to analyze RFET in a more complex circuit. We used Cadence Spectre as a commercial analog simulator and a table-based model of TIGFET in Verlog-A format from the NamLab group for simulation. Because the circuit-level simulation with table-based models is slow, we had to use various configurations for the Cadence tool to make the simulation faster.

We also did some simulations to analyze the capability of RFET in noise generation to enhance the side-channel resiliency of circuits against power attacks. The results show that by using RFET-based reconfigurable logic cells and a True Random Number Generator (TRNG), we can effectively randomize the power traces of the circuit to make the attack difficult. Besides, we performed simulations with our newly available table-based Verilog-A RFET model, which is compatible with 22nm FDSOI technology, to test the functionality of this model in SPICE simulation. Thus, we now have all the required SPICE simulation setup and results.

Task 1.5b: Conversion into liberty models for RFET/CMOS co-design

a) Goals

Creating a liberty library containing characteristics of the RFET cells. This library can be used by EDA tools for logic and Physical synthesis of RFET circuits.

b) Current States and Results

A liberty file contains information about standard cells, like the functionality of each cell and its timing and power consumption characteristics. To create the liberty file, all standard cells should be characterized. In the previous step, we characterized basic RFET cells manually (using DC and transient simulations using the Cadence Spectre analog simulator) and automatically (employing Cadence Liberate, a characterization tool, to automati-

cally do all required simulations and the liberty file generation process). Although the manual method is not scalable, it can be used to verify the automatic method. Manual and automatic ways of liberty file creation are shown in Figure 1.

In this step, we tested the latest version of the 22nm FDSOI-based RFET model in the SPICE simulation environment, and we characterized the logic cells with the target RFET model to generate the final liberty file. Besides, we added new complex standard cells to the library.

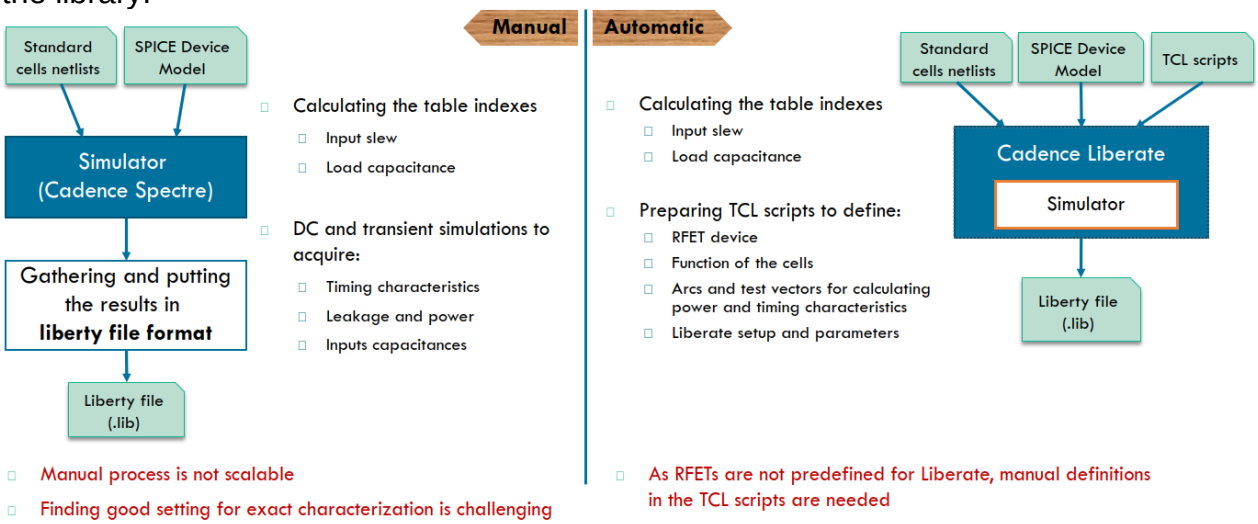

Figure 1. Manual and automatic liberty file creation procedure

Work Package WP 2: Synthesis and Design Automation

Task 2.1b: Creation of LEF libraries as a basis for layout for an RFET compatible EDA tool flow

a) Goals

Generating an abstract view and LEF library from the layout of the RFET-based standard cells.

b) Current States and Results

To provide a whole EDA flow, in particular physical synthesis for RFET-based ASIC design, creating both liberty and LEF library of standard cells is essential. LEF library contains two parts: Technology LEF and Cell LEF. The former includes the information related to technology, and the latter comprises the abstract information of the standard cells. The

layout of the standard logic cells, technology information, and abstract generator tool are required to generate the LEF library. Figure 2 shows the LEF file generation flow.
In the previous steps, we set up the LEF generation flow using the Cadence Abstract for RFET-based cells and generated the LEF library for the basic RFET-based logic cells (NAND, NOR, INV). Besides, we added the layout of some reconfigurable gates like XOR/XNOR and NAND/NOR cells and extracted their LEF files. As the reconfigurable gates are based on transmission gates, we added inverters and buffers inside some versions of these reconfigurable cells to make them compatible with other standard cells. Besides, in this new LEF, we have two versions with different heights for each cell.
In this step, we created the layouts of the new complex standard cells (e.g., AOI22) and added them to the LEF library.

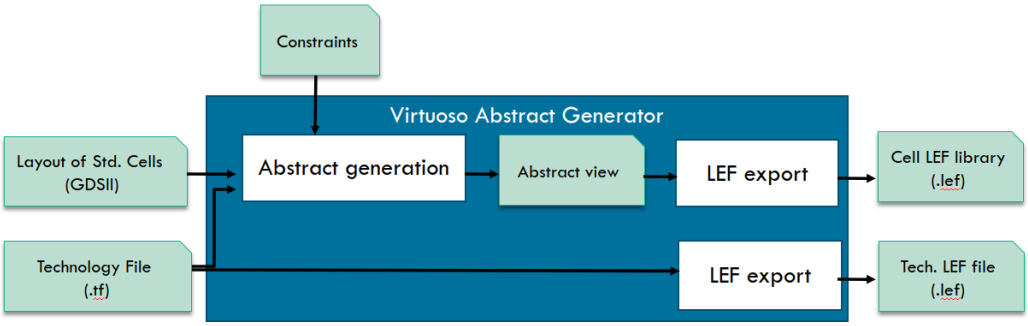

Figure 2. Physical (LEF) library generation procedure

Tasks 2.3a and 2.3b: Algorithms for placing RFET cells with a view to maximizing security with acceptable overhead

a) Goals

Providing security aware RFET placing with a view to minimizing the overhead.

b) Current states and results

Logic locking and layout camouflaging are two powerful techniques that security designers utilize to safeguard valuable IPs. Layout camouflaging protects the circuit from end users and test facility, while logic locking provides security against all the entities, even the untrusted foundry. Placing secure structures inside the circuits that bring protection against various classes of the attacks like SAT, structural, and fault injection is an open research problem. Designing such algorithms requires a careful flow that takes security into account, as well as the overhead that results from adding secured structures to the circuits. In our last report, we illustrated two algorithmic flows for layout camouflaging and logic locking. During our analysis, we realized that as layout camouflaging is easily translatable to a logic locking problem, any layout camouflaging scheme should provide security

against powerful structural and SAT attacks proposed to break logic locking techniques. As a result, regarding tasks 2.3a and 2.3b, we have been working on the implementation of logic locking flow illustrated in Figure 3.

Regarding logic locking flow, using RFET-based secure cells like XOR/XNOR can provide a good level of security with less impact on performance and area comparing CMOS. Generally, self-dual logic is the best candidate for RFET-based cells as it can be implemented as compact cells using the transistor-level reconfigurability of the RFETs. In our flow, the logic locking technique will be added to the circuit after the Generic mapping phase and before technology mapping. The reason is that we can preserve self-duality and structures that result in compact RFET-based secure structures by selecting suitable logic optimization algorithms. Like the camouflaging flow, the placement algorithm should utilize overhead and security feedback to provide the intended level of security and overhead for the circuit. In task 2.2b, we implemented a low overhead cell replacement technique to replace CMOS-based XOR and XNOR gates with RFET-based XOR/XNORs with the key signal as the function selector. For this task, we are expanding our replacement algorithm to include more dual cells that security designers can utilize based on their security and overhead tradeoffs. Moreover, for security evaluation, we have installed and run state-of-the-art structural attacks like MUXLink and OMLA, along with sequential and combinational open-source SAT attacks (NEOS). For technology mapping and power and delay analysis, we have selected the Cadence Genus synthesis tool that works well with the technology library prepared in previous tasks.

In this step, we completed the implementation of secure cell insertion algorithms based on Figure 3. for layout camouflaging and logic locking techniques.

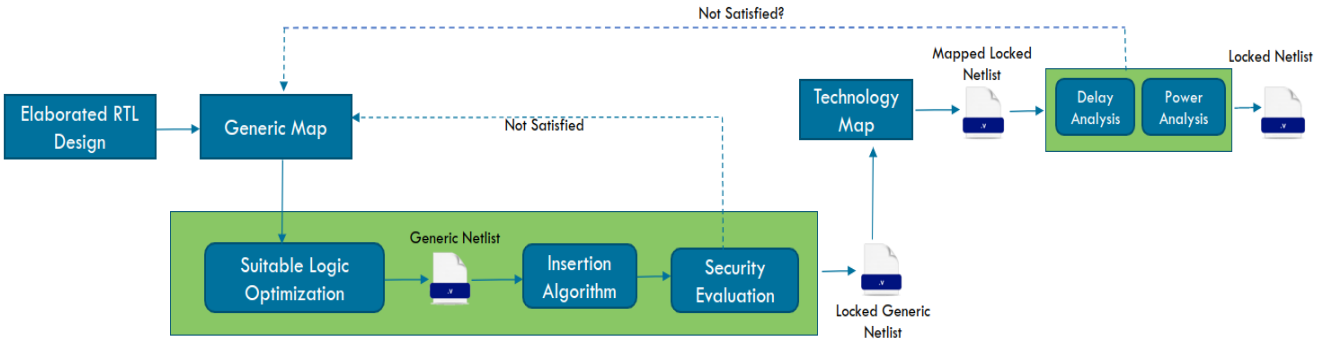

Figure 3. Proposed logic locking flow

Task 2.4a: Basic setup for physical synthesis

a) Goals

The aim is to set up a physical synthesis flow for RFET-based VLSI design.

b) Current States and Results

Having liberty and LEF files enables us to use commercial and open-source EDA tools for logic and physical synthesis. In the previous step, we set up Cadence Innovus, a physical synthesis tool, and did placement and routing steps for a CMOS-only design. The EDA flow for ASIC design is shown in Figure 4.
In this step, we tested the physical synthesis flow with the first version of our RFET-based LEF file developed in Task 2.1b. Based on our result, the RFET-based LEF is in the proper format and works well with the standard flow. Figure 5 shows the resulting layout of the circuit c1355 from the ISCAS'85 benchmark, which is synthesized using our LEF library.
As we provided the final liberty file for the 22nm-based RFET model in task 1.5b and added new complex cells to both liberty and LEF libraries in tasks 1.5b and 2.1b; in this step, we tested the whole synthesis flow with these final libraries.

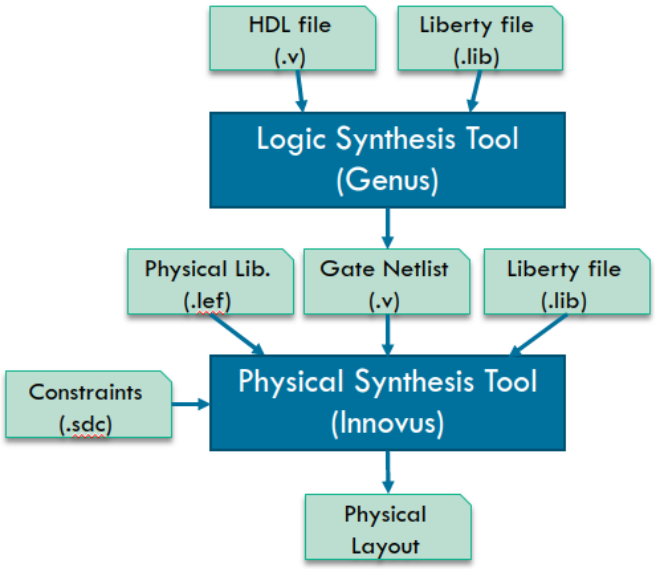

Figure 4. EDA flow for ASIC design

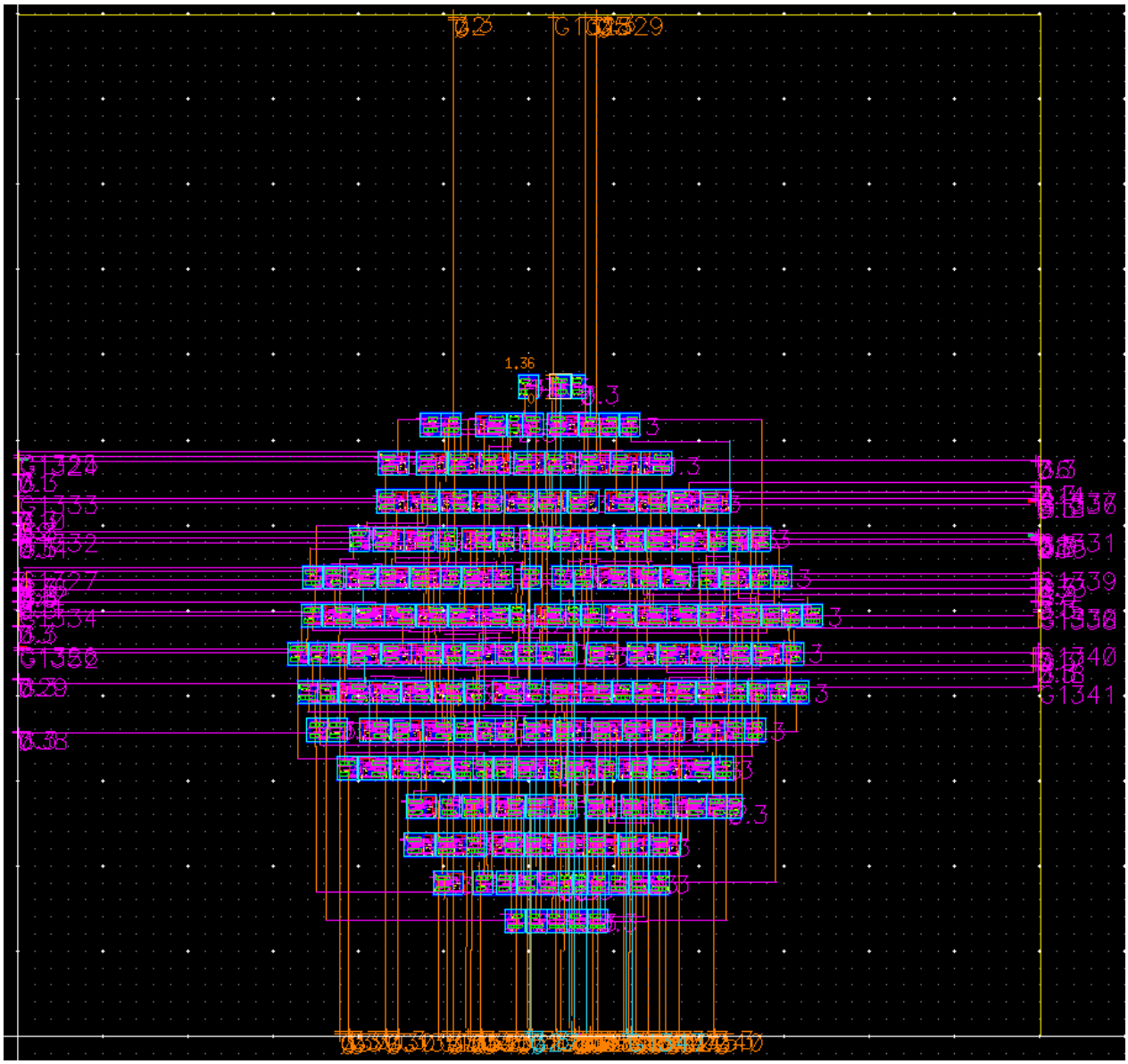

Figure 5. RFET-based layout of c1355 circuit

Task 2.4b: Physical synthesis of RFET safety cells in RFET / CMOS co-design

a) Goals

This task aims to provide a synthesis flow that enables the designer to do RFET/CMOS co-design.

b) Current States and Results

In tasks 2.3 and 2.4a, we have been implementing security flow and physical synthesis requirements for RFET-based secure circuits. For this task, we need to use our security-related replacement flow to decide on secure parts of the circuit that need to be implemented by RFET cells. Other parts of the circuits can be implemented using CMOS-based cells. To enable the circuit designer to use both RFET and CMOS cells (RFET/CMOS co-design), we should concatenate CMOS and RFET cell technology libraries (LEF and Lib) in a shared library. This way, our secure synthesis flow can utilize CMOS-based and RFET-based cells by analyzing the area, performance, power, and security of the circuit to achieve an optimized, secure circuit. In this step, we characterized the CMOS-based cells and created their layout. Then, we added this information to the RFET-based liberty and LEF libraries to enable our synthesis flow to select between RFET- and CMOS-based cells based on the required security or overhead aims.

Task 2.5a: Place, route of a virtual circuit demonstrator

a) Goals

The goal of this task is to show the correctness of the whole design flow, which is provided in the previous tasks.

b) Current States and Results

With the tools developed in tasks 1.1, 1.5, 2.1, 2.2, 2.3, and 2.4, it is now possible to place and route a complete circuit based on safe RFET cells. This EDA flow takes a circuit description in a hardware description language as input and outputs a chip layout. We selected well-known ITC'99 and ISCAS'85 benchmarks to demonstrate the functioning of the entire design flow.

Task 2.5b: Integration of the EDA environment in 22 nm FDSOI standard tool flow

a) Goals

This task aims to integrate the flow proposed in the previous tasks into an EDA environment, which supports 22nm FDSOI technology.

b) Current States and Results

We generated standard cell libraries for the RFET model (Tasks 1.5b and 2.1b), which are compatible with 22nm FDSOI technologies. These libraries follow standard formats supported by commercial and open-source EDA tools. As a result, our libraries and flow can be integrated into any standard EDA environment for 22nm FDSOI technologies. In this step, we integrated our flow with Cadence EDA tools.

Task 4.5: Comparison with CMOS protection circuits with regard to safety, area, performance and energy consumption

a) Goals

This task aims to compare the performance, area, and energy efficiency of a circuit secured by RFET-based cells with its CMOS-based implementation.

b) Current States and Results

In this task, we evaluated the possibility of providing an efficient and compact RFET-based secure design by implementing an 8x8 multiplier and compared the results with its CMOS-based counterpart. In this design, we used polymorphic RFET-based cells, which can be used in IP piracy techniques like logic locking, split manufacturing, and layout camouflaging. The comparison results are shown in Table 1.

Table 1 Comparison between CMOS- and RFET-based 8x8 multiplier

Technology	Delay (ps)	Power (nW)	PDP (aJ)	EDP (ps.aJ)	Area (UST)
CMOS (14 nm)	114.4	16.8	1.92	219.6	1950
RFET (GeNW 14nm)	183.9	5.8	1.06	194.9	1672.5

UST: Unit Size Transistor, PDP: Power Delay Product, EDP: Energy Delay Product

Task 4.6: Verwertungserkundung, Zertifizierungskonzept

a) Goals

This task aims to evaluate the feasibility of exploiting the results for manufacturability.

b) Current State

Global Foundries has already taped-out a couple of designs from the project. The data collected from these devices was used to refine the models that we have used in the other tasks of the project.

4. Zusätzliche Informationen

Die Antworten auf weitere Fragen finden Sie weiter unten.

a) die wichtigsten Positionen des zahlenmäßigen Nachweises

Die zwei Hauptkategorien, unter denen das Geld ausgegeben wurde, sind „Personal“ und „Reisen“. Die Ausgabe sind:
Personal: 419.230,85 EUR
Reisen: 9.900,30 EUR

b) die Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die durchgeführten Arbeiten entsprachen dem ursprünglichen Plan. Alle Arbeiten waren notwendig, um die Ziele des Projekts zu erreichen. Während des Projekts wurden keine zusätzlichen Mittel beantragt.

c) der voraussichtliche Nutzen, insbesondere die Verwertbarkeit des Ergebnisses – auch konkrete Planungen für die nähere Zukunft - im Sinne des fortgeschriebenen Verwertungsplans

Die Gruppe am Lehrstuhl für Prozessorentwurf der TU Dresden ist an den Lehrstuhl für Eingebettete Systeme der Ruhr-Universität Bochum gewechselt. Der neuen Gruppe an der Ruhr-Universität Bochum wurde ein Nachfolgeprojekt „Re-Design“ zugesprochen, dass die in diesem Projekt geleistete Arbeit fortführt. Die meisten Ergebnisse dieser Arbeit werden als Open-Source-Beiträge veröffentlicht und im neuen Projekt fortgeführt.

d) der während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordenen Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Andere Stellen im Projektbereich haben Fortschritte erzielt, die dem Zuschussempfänger während der Durchführung des Projekts bekannt wurden.
In [1] stellen die Autoren ein 10 nm Predictive Process Design Kit (PDK) für TIG-FETs vor, das validierte Designregeln und SPICE-Modelle enthält und erhebliche Flächenreduzierungen (26% für XOR-Gatter und 41% für Volladdierer) demonstriert. Das PDK unterstützt eine systematische Bewertung und umfasst Hardware-Sicherheitsanwendungen durch differenzielle Leistungsanalyse.
[2] beschreibt detailliert die RFET-Gerätephysik, aktuelle Optimierungen und stellt CMOS-artige und Transistor-reduzierte Standardzellen wie XOR-Gatter vor. Simulationen und Vergleiche mit der 180 nm SOI-Technologie heben Verbesserungen bei Antriebsstrom, N/P-Symmetrie und Schaltungsleistung hervor, wobei die Timing-Analyse auf komplexe Designs wie einen kryptografischen Beschleunigerkern ausgedehnt wird.

[3] Die Arbeit ist eine Erweiterung von [1], die eine neue Standardzellenbibliothek für 10-nm-Silizium-Nanodraht-TIGFET-Geräte einführt, die sowohl kombinatorische als auch sequentielle Gatter umfasst, um einen auf niedrigen Energieverbrauch optimierten RISC-V-Kern zu evaluieren. Das vorgeschlagene Design erreicht einen bis zu 4-fach geringeren Energieverbrauch bei Frequenzen bis zu 340 MHz und behebt parasitäre Effekte, die bei früheren Evaluierungen typischerweise übersehen wurden.
Die Arbeit in [4] erweitert [1] und [3] durch die Einführung einer Open-Source-Standardzellenbibliothek für Silizium-Nanodraht-TIGFETs, die effiziente XOR- und Majority-basierte Schaltungsdesigns ermöglicht. Unter Verwendung eines maßgeschneiderten Mixed-Logic-Syntheseansatzes weist der PicoRV-Kern eine 2,3-fache Flächenreduzierung und einen 5,7-fach geringeren Energieverbrauch im Vergleich zu herkömmlichen Designs auf.

[1] Gore, Ganesh, et al. "A predictive process design kit for three-independent-gate field-effect transistors." *2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2019.
[2] Reuter, Maximilian, et al. "From mosfets to ambipolar transistors: Standard cell synthesis for the planar rfet technology." *IEEE Transactions on Circuits and Systems I: Regular Papers* 68.1 (2020): 114-125.
[3] Keyser, Michael, Roman Gauchi, and Pierre-Emmanuel Gaillardon. "An energy-efficient three-independent-gate fet cell library for low-power edge computing." *2022 IFIP/IEEE 30th International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2022.
[4] Gauchi, Roman, Ashton Snelgrove, and Pierre-Emmanuel Gaillardon. "An open-source three-independent-gate fet standard cell library for mixed logic synthesis." *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2022.

e) die erfolgten oder geplanten Veröffentlichungen des Ergebnisses nach Nr. 5 der NKBF/NABF

Nachfolgend finden Sie die Liste der Veröffentlichungen, die aus diesem Projekt hervorgegangen sind.

- Kavand, N., Darjani, A., Chhabra, G., & Kumar, A. (2024, July). RFET-Based Dynamic Differential Logic Cells Against Power Side-Channel Attacks. In *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (pp. 136-142). IEEE.
- Nima Kavand, Armin Darjani, Giulio Galderisi, Jens Trommer, Thomas Mikolajick, Akash Kumar, "REDCAP: Reconfigurable RFET-based Circuits Against Power Side-Channel Attacks" (to appear), *In Proceeding: 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2024

- Niladri Bhattacharjee, Viktor Havel, Suruchi Kumari, Nima Kavand, Jorge Navarro Quijada, Akash Kumar, Thomas Mikolajick, Jens Trommer, "Dynamic Reconfigurable Security Cells based on Emerging Devices Integrable in FDSOI Technology" (to appear), *In Proceeding: 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2024
- Armin Darjani, Nima Kavand, Shubham Rai, Akash Kumar, "Thwarting GNN-based attacks against logic locking", In IEEE Transactions on Information Forensics and Security, Institute of Electrical and Electronics Engineers (IEEE), pp. 1–1, 2024.
- Nima Kavand, Armin Darjani, Shubham Rai, Akash Kumar, "Design of Energy-efficient RFET-based Exact and Approximate 4:2 Compressors and Multipliers", In IEEE Transactions on Circuits and Systems II: Express Briefs, pp. 1-1, May 2023
- Jens Trommer, Niladri Bhattacharjee, Thomas Mikolajick, Sebastian Huhn, Marcel Merten, Mohammed Elkacem Djeridane, Muhammad Hassan, Rolf Drechsler, Shubham Rai, Nima Kavand, Armin Darjani, Akash Kumar, Violetta Sessi, Maximilian Drescher, Sabine Kolodinski, Maciej Wiatr, "Design Enablement Flow for Circuits with Inherent Obfuscation based on Reconfigurable Transistors", In Proceeding: Design, Automation and Test in Europe Conference (DATE), IEEE/ACM, April 2023
- Nima Kavand, Armin Darjani, Shubham Rai, Akash Kumar, "Securing Hardware through Reconfigurable Nano-structures", In Proceeding: International Conference on Computer-Aided Design (ICCAD), ACM/IEEE, Nov 2022
- Armin Darjani, Nima Kavand, Shubham Rai, Mark Wijtvliet, Akash Kumar, "ENTANGLE: An Enhanced Logic-locking Technique for Thwarting SAT and Structural Attacks", In Proceeding: ACM Great Lakes Symposium on VLSI (GLSVLSI), 6/2022.