Luis Antonio Quispe Cartagena

Sensor de temperatura na tecnologia CMOS para proteção de CIs: arquitetura e aplicações

São Paulo

2020

Luis Antonio Quispe Cartagena

Sensor de temperatura na tecnologia CMOS para proteção de CIs: arquitetura e aplicações

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Mestre em Ciências.

São Paulo

2020

Luis Antonio Quispe Cartagena

Sensor de temperatura na tecnologia CMOS para proteção de CIs: arquitetura e aplicações

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Mestre em Ciências.

Área de Concentração:
Microeletrônica

Orientador
Prof. Dr. Walter Jaimes Salcedo e
Prof. Dr. Silvio Ernesto Barbin (*in memoriam*)

São Paulo

2020

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, _____ de _____ de _____

Assinatura do autor: _____

Assinatura do orientador: _____

Catalogação-na-publicação

Cartagena, Luis
Sensor de temperatura na tecnologia CMOS para proteção de CIs: arquitetura e aplicações / L. Cartagena -- versão corr. -- São Paulo, 2020.
72 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1.CMOS 2.Sensor de temperatura 3.Ataques de mal funcionamento 4.Cartões inteligentes 5.Circuito integrado I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II.t.

Este trabalho é dedicado a meus pais e irmãos.

AGRADECIMENTOS

A Deus por iluminar o meu caminho nesta maravilha de vida e permitir a realização deste trabalho.

A minha mãe Julia por me ensinar a coragem de ser invencível aos golpes da vida. Ao meu pai Simon por sempre ter acreditado e se orgulhado de mim. Aos meus irmãos Gregoria, Lidia, Salvador, Graciela, Edelina, Fredy, Yesica, Juana e José, pelos momentos gratos.

Eu também gostaria de agradecer aos meus professores que foram verdadeiros alicerces na longa estrada inesgotável por estudar. Aos meus colegas e amigos brasileiros e peruanos que conheci no Brasil, que ajudaram, tanto profissional quanto pessoalmente, em numerosas ocasiões.

Ao meu orientador Prof. Dr. Walter Jaimes Salcedo, pela orientação e mais do que isso por sempre ter acreditado em mim, mesmo quando eu não enxergava meus passos. Minha maior admiração pelas grandes qualidades como pessoa, atitudes e exemplar profissional.

Um agradecimento especial ao amigo e Prof. Dr. Silvio Ernesto Barbin, que estará sempre em nossos corações, imortalizado por sua obra, sua excelência profissional, sua dedicação ao ensino e sua personalidade tão marcante e inesquecível. Barbin, é muito difícil ficar sem nossas conversas técnicas mirabolantes, os papos sobre suas histórias maravilhosas da suas viajes pelo mundo. Onde quer que você esteja, desejo que você possa ver e se emocionar com as sementes que você plantou em vida, enquanto elas nascem, crescem e florescem como suas tão queridas primaveras. Obrigado por toda a confiança, amizade, carinho e por permitir que eu tenha participado de tantas coisas de sua vida e de sua família. Lutarei por fazer tudo aquelo que você tinha planejado para continuar com a pesquisa. Até um dia meu amigo.

E finalmente, à Universidade de São Paulo (USP) pela oportunidade de fazer este curso e a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pela concessão da bolsa de mestrado.

"Só sei que alguma coisa sei, que não sei o quê que é".
(Antonio, Q; vidas Invisíveis)

RESUMO

Luis Q. Cartagena. **Sensor de temperatura na tecnologia CMOS para proteção de CIs: arquitetura e aplicações**. 2020. 72 p. Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo, São Paulo, 2020.

Neste trabalho de pesquisa é apresentado os resultados do projeto de um sensor de temperatura de baixa potência para a proteção de cartões inteligentes de ataques a sua segurança nos extremos da faixa de temperatura operacional. Os ataques geralmente utilizam técnicas de geração de falhas que normalmente aparecem em condições ambientais anormais tal como o estado de elevada temperatura, provocando assim o mau funcionamento do processador no cartão inteligente, permitindo o acesso adicional à informação. O objetivo deste projeto foi o desenvolvimento de um sistema de proteção do chip de cartões inteligentes desta arte de adulteração de segurança para a faixa de temperatura de $-20\,°C$ a $120\,°C$ para tal fim foi projetado um sistema sensor de temperatura de área pequena e de baixo consumo de energia. O sensor foi projetado em Cadence usando o conceito *System-on-a-Chip* (SoC) na tecnologia padrão CMOS de $0{,}18\,\mu m$ (TSMC) e opera com uma tensão de alimentação de $1{,}2\,V$. O Sensor de temperatura é baseado em um circuito com dois transistores CMOS (*Complementary Metal Oxide Semicondutor*) e um transistor bipolar PNP para produzir uma tensão CTAT (*Complementary To Absolute Temperature voltage*). O resultado obtido da simulação do sensor de proteção de temperatura nos limites de uma faixa de temperatura de $-40\,°C$ a $140\,°C$ e $V_{dd} = 1{,}2\,V \pm 10\%$, mostraram um excelente desempenho para o sensor; com uma taxa de rejeição da fonte de alimentação PSRR (*Power supply rejection ratio*) de $-62\,dB$ no pior dos casos e com histerese de $5\,mV$. Este novo *design* de circuito pode efetivamente funcionar como um excelente protetor contra adulteração de segurança em cartões inteligentes.

Palavras-Chave: CMOS. Sensor de temperatura. Ataques de mal funcionamento. Cartões inteligentes. Circuito integrado.

ABSTRACT

Luis Q. Cartagena **CMOS technology temperature protection sensor for ICs: architecture and applications**. 2020. 72 p. Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo, São Paulo, 2020.

In this research work, it is presented the results of the design of a low-power temperature sensor for the protection of smart cards from attacks to its security at the extremes of the operating temperature range. The attacks usually use failure generation techniques that normally appear in abnormal environmental conditions such as the high temperature state, thus causing the processor to malfunction in the smart card, allowing additional access to information. The objective of this work was to development of a smart card chip protection system of this security tampering art for the temperature range from $-20\,^{\circ}\mathrm{C}$ to $120\,^{\circ}\mathrm{C}$, for this purpose, was designed a temperature sensor system of small area and low power consumption. The sensor was designed in Cadence using the *System-on-a-Chip* (SoC) concept employing standard CMOS technology of 0,18 µm (TSMC) and operates on a supply voltage of 1,2 V. The temperature sensor is based on a circuit with two CMOS transistors (*Complementary Metal Oxide Semiconductor*) and a PNP bipolar transistor for producing a CTAT voltage (*Complementary To Absolute Temperature voltage*). The result obtained from the simulation of the temperature protection sensor at the limits of a $-40\,^{\circ}\mathrm{C}$ to $140\,^{\circ}\mathrm{C}$ temperature range and $V_{dd} = 1{,}2\,\mathrm{V}\ \pm 10\%$, showed an excellent performance for the sensor; with a Power Supply Rejection Rate (PSRR) of $-62\,\mathrm{dB}$ in the worst case and with hysteresis of 5 mV. This new circuit textit design can effectively work as an excellent protector against security tampering on smart cards.

Key-words: CMOS. Temperature sensor. Malfunction attacks. Smart cards. Integrated circuit.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BJT	*Bipolar Junction Transistor*
CI	Circuito Integrado (*Integrated Circuit*)
CMOS	*Complementary Metal-Oxide-Semiconductor*
CTAT	Complementa a temperatura absoluta (*Complementary To Absolute Temperature*)
EMV	*Europay, MasterCard Visa*
GSM	*Global System for Mobile Communications*
ICC	*Integrated Circuit Card*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
OTP	*Over Temperature Protection*
PTAT	Proporcional a temperatura absoluta (*Proporcional To Absolute Temperature*)
PSRR	Razão de rejeição ao ruído da fonte (*Power Supply Rejection Ratio*)
SCC	*Smart Card Center*
SE	*Secure Element*
SIM	*Subscriber Identity Module*
SoC	*System-on-a-Chip*
V_T	*Thermal Voltage*

SUMÁRIO

1 INTRODUÇÃO

Na atualidade um dos Circuitos Integrados (CIs) mais utilizados são os cartões inteligentes (*Smart Card*). Estes sistemas são empregados em um grande número de aplicações em telecomunicações móveis como GSM (Global System for Mobile Communications), em serviços bancários, dentre outros. Seu uso vem crescendo cada vez mais, mas na parte de proteção de dados nem todos os CIs são ainda são bem-sucedidos (WITTEMAN, 2002). Estes podem ser atacados de três maneiras diferentes: ataques lógicos, ataques físicos e ataques de canais laterais. Dentre os ataques de canais laterais, um dos mais comuns é a variação de temperatura nos extremos da faixa de operação, pois CIs são vulneráveis a condições ambientais anormais. Estas causam mau funcionamento do processador, permitindo um acesso adicional à informações pessoais almacenadas no cartão (BAR-EL et al., 2006). Dentre os ataques físicos, um dos mais comuns é de *microprobing*, é um ataque invasivo que exigem a destruição do pacote de CI, assim tendo um acesso direto no layout do CI (SHI et al., 2016), para fazer engenharia reversa e entender a estrutura interna do CI sob investigação e o estabelecimento de conexões elétricas com os fios de sinal do circuito ou para realizar medições intensivas. Portanto, é necessário desenvolver algum tipo de proteção térmica e resistiva a adulteração.

A maneira mais comum de defesa contra esse tipo de ataques é o uso de sensor de temperatura e uma malha resistiva a adulteração sendo estos posicionados de maneira estratégica no CI a fim de garantirem uma maior seguridade. Os sensores térmicos mais conhecidos são quatro; sensor termopar, detector resistivo de temperatura (RTD) de platina, termistor e sensor BJT. Mas na tecnologia CMOS, o circuito usa um diodo de junção PN ou um transistor bipolar PNP conectado na configuração de diodo. A saída do circuito sensor na tecnologia CMOS pode ser uma tensão ou uma corrente, segundo a configuração do tipo *Complementary To Absolute Temperature* (CTAT) ou *Proporcional To Absolute Temperature* (PTAT). Para o circuito de proteção de ataques de adulteração é implementado na camada superior do CI através de uma malha de resistências, como uma chave baseada na taxa de variação do nível de tensão na resistência.

A proteção de temperatura e resistivo a adulteração é um recurso de interface que avisa ao bloco sequenciador sobre eventos de falha. Se a temperatura for mais baixa que o extremo inferior ou mais alta que o extremo superior da faixa de temperatura de operação ($-20\,^{\circ}\mathrm{C}$ a $120\,^{\circ}\mathrm{C}$) e a resistência for maior a $150\,\mathrm{K}\Omega$, uma sequência de desativação é iniciada e começa a proteger o cartão. A tensão no terminal ON fica alta, para informar o microcontrolador sobre a existência de falha de temperatura ou resistência.

1.1 Motivação

Os sensores de temperatura desempenham um papel importante na indústria e na área de pesquisa, como no controle de temperaturas de processo, reações químicas e também para uso na agricultura. Outras aplicações importantes dos sensores de temperatura incluem a medição da temperatura do tecido corporal. Por esse motivo, os sensores de temperatura são importantes na integração em dispositivos portáteis para muitas aplicações.

Um dos desafios encontrados no projeto de cartões inteligentes (*smart cards*) é a implementação de técnicas de proteção térmica para atingir as necessidades abordadas anteriormente. A pesquisa desenvolvida apresenta uma técnica nova de proteção térmica para cartões inteligentes, que protege eficazmente o circuito de ataques de segurança. Para tratar as vulnerabilidades dos CIs, pesquisadores tem desenvolvido metodologias para proteção de ataque de canal lateral (WANG et al., 2013; KIM et al., 2017), mas o campo de estudo é ainda bastante abrangente pois a cada dia surgem novas formas de adulterar os CIs.

Neste projeto, é desenvolvido um sensor de temperatura destinado a evitar ataques de adulteração para proteção de cartões inteligentes na faixa de $-20\,^{\circ}\mathrm{C}$ a $120\,^{\circ}\mathrm{C}$ que é a faixa de temperatura de funcionamento do CI. Um dos objetivos é projetar o circuito em uma área pequena, além de ser de baixo consumo de energia e ser integrado no CI. O sensor é projetado utilizando-se o software Cadence usando o conceito *System-on-a-Chip* (SoC) (KLAAS, 2004) para tecnologia CMOS padrão 0,18 µm TSMC, operando com tensão de alimentação de 1,2 V.

1.2 Antecedentes históricos

Atualmente, os Circuitos Integrados (CIs) são usados não apenas para controlar sistemas, mas também para protegê-los contra ameaças de segurança. Uma batalha contínua é travada entre fabricantes que desenvolvem novas soluções de segurança, aprendendo suas lições com erros anteriores e a comunidade de *hackers*, constantemente tentando quebrar as proteções implementadas. Um dos CIs mais usados na atualidade com numerosas aplicações futuras são os cartões inteligentes (REPORT, Augost 2018), os quais são os mais atacados para recuperação de seus algoritmos de segurança e materiais de criptografias armazenados. Podemos distinguir cinco principais categorias de ataque (TEHRANIPOOR; WANG, 2011; MAYES; MARKANTONAKIS, 2017): *Microprobing*, Engenharia reversa, Geração de Falhas, Ataques de software e Ataques de canal lateral. Todas as técnicas de *microprobing* e engenharia reversa são ataques invasivos. Eles exigem laboratórios especializados e no processo destroem a embalagem. Os outros três são ataques não invasivos, o dispositivo atacado não é fisicamente danificado durante esse ataque.

Para minimizar esses ataques foram desenvolvidos circuitos de proteção como: a implantação de uma resistência dinâmica de diodos para redução da tensão de ruptura (MAES; SIX; SANSEN, 1981), análise de um dispositivo integrado de disjuntor para proteção de circuitos eletrônicos de baixa potência (LAUR et al., 1999), driver de porta para transistor bipolar de gate isolado (TBGI), para a ativação de dois níveis para reduzir a corrente de pico ao ligar o dispositivo, e a desativação de dois níveis para limitar a sobretensão quando o dispositivo está desligado (DULAU et al., 2006).

A proteção de CI de cartão inteligente dos ataques como *microprobing* tornaram-se uma preocupação séria. Um invasor pode remover camadas de materiais e expor os fios que contêm informações críticas de segurança (SHI et al., 2016). Mostra-se que esses ataques podem ser práticos em chips reais, se a criptografia de memória não é tão boa quanto deveria ser. Foi possível extrair toda a memória de um microcontrolador seguro de 8 bits com apenas 8 agulhas de medição (SKOROBOGATOV, 2017). O propósito deste tipo de ataque é acessar diretamente os fios internos de um módulo crítico de segurança e extrair informações confidenciais em formato eletrônico.

Microprobing, convinado com a técnica de engenharia reversa (QUADIR et al., 2016) e edição de circuito, representa uma séria ameaça às aplicações críticas da missão e, portanto, exige o desenvolvimento de contramedidas eficazes da comunidade de pesquisa (WANG et al., 2017). Pesquisas feitas contra estes tipos de ataques físicos reportam que confiar nos procedimentos de proteção à adulteração é problemático; cartões inteligentes são quebrados rotineiramente, e até mesmo um dispositivo que foi descrito por um governo sinaliza a agência como "o processador mais seguro geralmente disponível" acaba por ser vulnerável (ANDERSON; KUHN, 1996; ANDERSON; KUHN, 1997; KÖMMERLING; KUHN, 1999), e com construir dispositivos resistentes à adulteração e usá-los efetivamente é muito mais difícil do que parece.

Detalhes em relação à *Geração de Falhas* mostram experimentalmente que os cartões inteligentes protegidos são vulneráveis (WOUDENBERG; WITTEMAN; MENARINI, 2011). Usam condições ambientais anormais para gerar avarias no dispositivo que fornecem acesso adicional (SKOROBOGATOV, 2005; TEHRANIPOOR; WANG, 2011) para extração de dados. O trabalho (HUTTER; SCHMIDT, 2013) incentiva a conscientização de ataques baseados em temperatura que são conhecidos há anos, mas não são bem descritos na literatura. Ele também serve como ponto de partida para futuras investigações de pesquisa.

Vendo estes acontecimentos muitas empresas vítimas como TV, Bancos, etc. Estão investindo na segurança, um das várias formas de segurança em geração de falhas, é a proteção em temperatura devido a que nos CIs, as condições ambientais anormais permitem acesso adicional a informações. Os sensores de Temperatura baseados no processo CMOS (BAKKER; HUIJSING, 1996), desde sua criação vem sendo um dos dispositivos importantes

com variedade de aplicações não só para proteção em temperatura mas também para dispositivos de prevenção de saudê dentre outros (LAW; BERMAK; LUONG, 2010; RAO et al., 1997; GARULLI et al., 2017; DAVIDSON; BUIS; GLESK, 2017; DESCENT; IZQUIERDO; FAYOMI, 2018; YANG et al., 2019).

Esta pesquisa apresenta a implementação de uma nova arquitetura de sensor de temperatura para proteção em temperatura e uma malha resistiva contra a adulteração do CI, de baixo consumo de energia e de pequena área, para ser aplicado na proteção de cartões inteligentes *Smart Cards*, sendo estos integrados no mesmo circuito para melhor controle deste arte de adulteração.

1.3 Objetivos

O objetivo central da pesquisa para esta dissertação é a proposta de um sensor de temperatura e um sensor resistivo para proteção do CI de cartões inteligentes (*Smart Cards*) de ataques geradas de falhas para condições ambientais anormais e de ataques de adulteração, e ser integrado dentro do CI. Os passos iniciais serão mostrar os tipos de ataques à segurança em CI de cartões inteligentes (*Smart Cards*). Para proteção de ataques geradas de falhas em condições ambientais anormais, foi projetado um sensor de temperatura na tecnologia CMOS e para os ataques de adulteração foi projetado um sensor resistivo a adulteração. Além de se projetar os sensores de proteção de CI de cartões inteligentes desta arte de adulteração, foi necessário criar os sensores com uma pequena área e de baixo consumo de energia.

1.4 Desafios

Um dos grandes desafios é o desenvolvimento de estratégias de proteção contra ataques, incluindo adulteração e ataques de temperatura. A adulteração é usada para engenharia reversa e os ataques de temperatura normalmente resultam no mau funcionamento de um processador de cartão inteligente, permitindo acesso indevido à informação.

A principal contribuição deste trabalho é a implementação de um sensor de temperatura para a proteção de ataques geradas de falhas nos limites do funcionamento do CI e um sensor resistivo para a proteção de ataques invasivos, integrado no circuito de um *Smart Card*. Os sensores utilizam a própria alimentação do CI para melhor controle de ativação e desativação do mesmo.

1.5 Estrutura da dissertação

Este documento é organizado em 5 capítulos incluindo esta introdução, da seguinte maneira:

Capítulo 2 – Sensores de Temperatura e Cartões Inteligentes. Este capítulo descreve uma abordagem sobre a importância dos cartões inteligentes (*Smart Cards*), aplicações e ataques que sofrem os CIs. Para propor uma solução contra este tipo de adulteração, se fez também uma revisão dos transistor BJT e CMOS, seus comportamento com a temperatura para projetar o sensor de temperatura na tecnologia CMOS.

Capítulo 3 – Arquitetura de Sensor de Temperatura e Resistência a Adulteração. Neste capítulo contém as principais descrições de cada bloco a projetar os circuitos protetores, considerações e conceitos relativos ao sensor de temperatura e resistência a adulteração em CMOS. Na sequência, são apresentadas análises e discussões.

Capítulo 4 – Análises dos resultados. Nesta seção, apresenta-se o processo de *design* de CI em CMOS, como um conjunto para o qual se usa o diagrama de blocos mostrado na Figura A.1, encontram-se com a análise dos resultados, a metodologia empregada e discussões das medidas.

Capítulo 5 – Conclusões e Trabalho Futuro. Neste capítulo, revisamos os principais resultados apresentados nesta dissertação e descrevemos futuras investigações relacionadas a esses resultados.

2 SENSORES DE TEMPERATURA E CARTÕES INTELIGENTES (*SMART CARDS*)

Neste capítulo, descreve-se uma abordagem sobre os cartões inteligentes (*Smart Cards*). Introduz-se o estado de arte sobre cartão inteligente, sua classificação nos diferentes níveis através de um diagrama de blocos, para em seguida identificar os tipos de cartões inteligentes, e suas principais aplicações atuais. A discussão é estendida para a segurança e tipos de ataques e finalmente enfatiza-se os tipos de proteção existentes em cartões inteligentes, para propor o desenvolvimento de sensores de proteção deste tipo de ataques.

Para propor o desenvolvimento de sensor é necessário a compreensão dos transistores BJT e CMOS, variação com a temperatura, alguns tipos de sensores de temperatura. Começamos discutindo alguns dos enunciados.

2.1 Cartões inteligentes

O cartão inteligente foi inventado e patenteado na década de 70. No entanto, o termo **cartão inteligente** não foi bem estabelecido até a década de 80, quando a França iniciou uma grande campanha para exportar a tecnologia. No final de 1993, a EMV (*Europay*, *MasterCard* e *Visa*) tomou a iniciativa de desenvolver especificações de Serviços de Pagamento da ICC (*Integrated Circuit Card*), um ano depois a EMV lançou uma primeira versão do projeto. Após o conceito ter sido aceito, nos últimos anos, começou seu uso em grande variedade de aplicações. Na atualidade, novos desenhos ambiciosos de circuitos em silício e encriptações estão sendo estudados (maiores informações na seção 2.1.3 de aplicações atuais para cartões inteligentes).

Um cartão inteligente é um cartão de plástico com tamanho padrão ISO/IEC [1] 7810 (tamanho e espessura do cartão bancário), que contém CIs dentro de seu corpo, como na ilustração da Figura 2.1 (HENDRY, 2007).

Um cartão inteligente pode armazenar uma quantidade significativa de dados e realizar operações básicas de computação. Este cartão pode incluir também uma cadeia magnética ou, um código de barra. De longe, parece um cartão de crédito com uma pequena placa de metal na frente. Essa placa, é a interface elétrica de um computador ínfimo e altamente integrado, com uma matriz de 8 contatos e localizado no micro módulo

[1] ISO/IEC são significativos para os cartões inteligentes, pois definem as propriedades básicas delas. ISO (*International Organization for Standardization*) é uma Organização Internacional para Normalização, encargada de aprovar padrões internacionais em diversas áreas; enquanto IEC (*International Electrotechnical Commission*) é a Comissão Eletrotécnica Internacional encargada de aprovar padrões referente a tecnologias elétricas, eletrônicas e relacionadas(RANKL; EFFING, 2004).

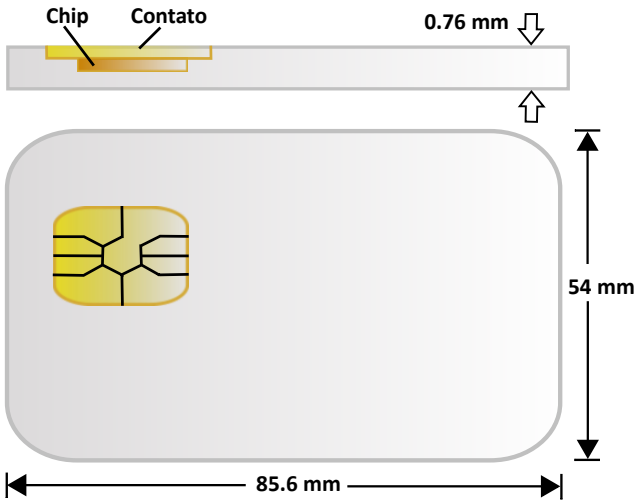


Figura 2.1 – Detalhes do dimensionamento do cartão bancário que contem um CI de acordo ao padrão ISO/IEC 7816.

Fonte: Elaborado pelo autor.

de acordo ao padrão ISO/IEC 7816[2]; mas só 6 dos quais são normalmente conectados para o chip. Os contatos fornecem energia ao chip via Vcc/GND, à linha de comunicação I/O, além de linhas clock (CLK) e reset (RST).

Na Figura 2.2 O pino Vpp era usado para reprogramar a memória EEPROM, mas na atualidade não sendo usado ao igual que os dos pinos inferiores D+ e D-, quedando como reservados para usos futuros (*Reserved for Future Use* - RFU), alguns cartões e leitores utilizam apenas os seis contatos superiores. No entanto, algumas indústrias já padronizaram o uso dos antigos contatos RFU e Vpp para novos serviços.

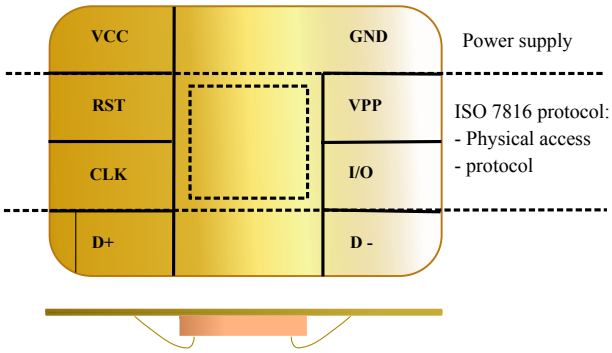


Figura 2.2 – Placa metal padrão de contatos com cartão inteligente de acordo ao padrão ISO/IEC 7816.

Fonte: Elaborado pelo autor.

[2] Os padrões ISO/IEC são especialmente significativos para cartões inteligentes, Fonte: <https://www.iso.org/obp/ui/> Acesso em 30 de maio de 2018.

A introdução do cartão SIM (*Subscriber Identity Module*) baseado no cartão inteligente utilizado em equipamentos de telefonia móvel GSM na Europa foi a principal revolução no uso destes cartões (RANKL; EFFING, 2004).

Assim, o grande emprego nos diferentes perfis de cartões inteligentes, tais como, documentos de identificação (IDs), passaportes, cartões de crédito e bilhetes eletrônicos; os tornaram importantes no uso popular. Os candidatos que poderiam ser descritos como cartões inteligentes são, portanto, numerosos e, assim, nossa definição será refinada um pouco para eliminar alguns dos menos relevantes. Desse modo, um cartão inteligente:

(i) Tem um identificador único;
(ii) Pode participar de uma transação eletrônica automatizada;
(iii) É usado principalmente para adicionar segurança;
(iv) Não é facilmente burlado ou copiado, em apoio a (ii) e (iii);
(v) Pode armazenar dados de forma segura;
(vi) Pode hospedar/executar uma variedade de algoritmos e funções de segurança.

Nessa situação, esta definição será aplicada a alguns tipos de cartões bem conhecidos, para constatar se eles podem ser classificados realmente como inteligentes. Por último é importante mencionar que, a tecnologia está sempre em constante evolução e hoje o SCC (*Smart Card Centre*) que é um centro mundial de excelência para treinamento e pesquisa em questões de segurança associadas a cartões inteligentes, tokens e dispositivos móveis; está interessado em abordagens de segurança, tais como NFC (*Near-Field Communication*) comunicação por campo de proximidade de dispositivos móveis (telefones), segurança veicular (transporte), nos desafios recentes em IoT (*Internet of Things*), e infraestruturas, em geral. Nesse cenário, esta área de segurança de cartões inteligentes tem uma importância muito relevante dentro desta proposta de projeto de pesquisa.

2.1.1 Classificação de cartões

Os cartões inteligentes, podem ser classificados segundo o diagrama mostrado na Figura 2.3, onde, o nível superior inclui todos os tipos de cartões, que podem ter vários formatos. Logo, estes podem ser divididas em cartões sem chips e cartões com chips. Consequentemente, esse último tipo chamado de cartões com chip, são conhecidos como cartões inteligentes. É o chip, o elemento distintivo essencial; pode ser um chip de memória, então o cartão é chamado de cartão de memória ou chip de microcontrolador, então o cartão é chamado de cartão de processador. As placas com processador podem ser divididos em placas com ou sem co-processadores para executar algoritmos criptográficos assimétricos como RSA (*Rivest, Shamir e Adleman*) ou algoritmos criptográficos de curva elíptica (*Elliptic Curve Cryptosystems* – ECC) (RANKL, 2007).

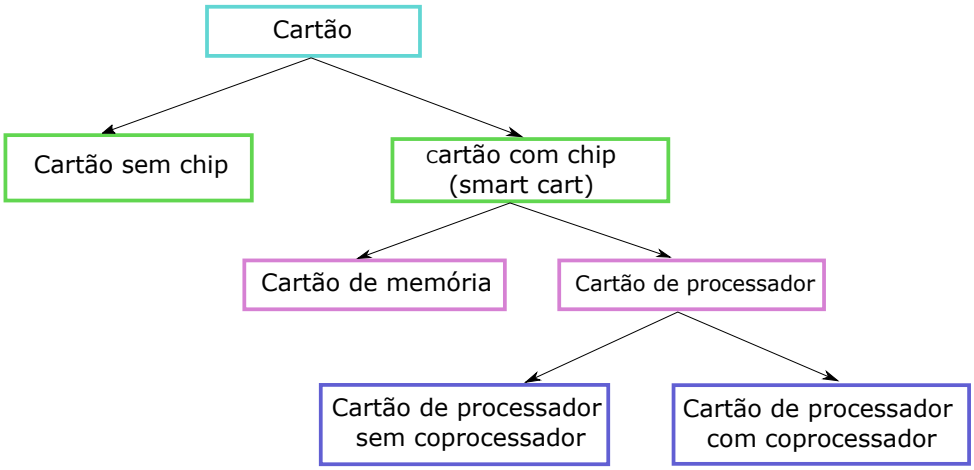


Figura 2.3 – Classificação de cartões com e sem chips.

Fonte: Elaborado pelo autor.

Essa classificação fornece uma visão geral adequada dos tipos de cartões mais usados, mas também, pode ser estendida para incluir dispositivos que usam tecnologia de cartão inteligente. Os exemplos, mais conhecidos de tais dispositivos são *super smart cards* e *tokens*. Uma super *smart card* tem uma interface de usuário direta para o microcontrolador de cartão inteligente, na forma de elementos de cartão adicionais, como uma tela e botões. Já um *token* pode ser considerado como um dispositivo personalizado que possui toda a segurança útil, do que o cartão usual. Exemplos típicos incluem *token* na forma de plugues USB que podem ser conectados diretamente a um PC. No entanto, a tecnologia subjacente permanece a mesma dos cartões inteligentes, com apenas a aparência diferente.

Pode-se cair na suposição que todos os cartões com chip são mais seguros do que os cartões com placa magnética e que a presença dos contatos dourados implica que se trata de um cartão inteligente. Essas suposições são incorretas e perigosas. O cartão com chip mais simples pode conter um único valor fixo, o protocolo de aplicação seria simplesmente ler este valor fixo para comparação. Seria fácil para um invasor ler o valor de um cartão válido e produzir uma cópia e, assim, esse tipo de cartão falha na nossa quarta definição de cartão inteligente da mesma maneira que o cartão com placa magnética.

Cartões com Chip de memória

Cartões baseados em memória precisam de um leitor de cartão para manipular os dados no cartão. Eles se comunicam com o leitor usando alguns protocolos síncronos. Este tipo de cartões não tem poder de processamento e não podem gerenciar os dados armazenados neles. Geralmente é uma EEPROM, que é acessada usando uma lógica sequencial, e também é possível incorporar algoritmos de segurança simples, como pode-se observar na Figura 2.4 (a). A flexibilidade de aplicação é altamente limitada, mas, do

lado positivo, os cartões de memória são muito econômicos. Por essa razão, os cartões de memória são usados em aplicações de grande escala e sensíveis a preço.

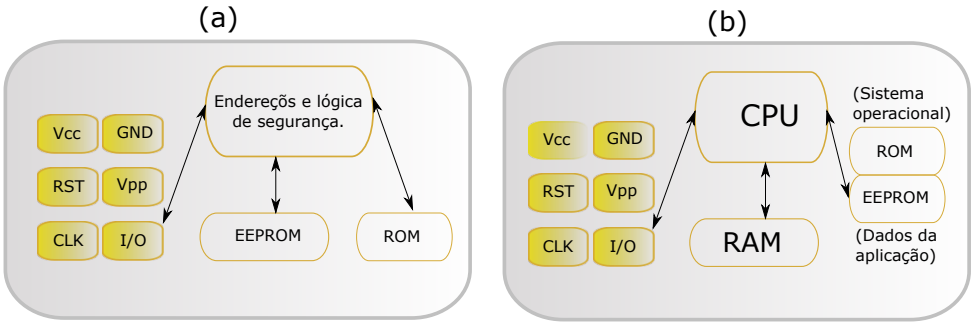


Figura 2.4 – Cartões com chip, com e sem microprocessador: (a) Arquitetura típica de um cartão apenas com chip de memória e (b) Arquitetura típica de um cartão com chip de microprocessador e memória.

Fonte: Elaborado pelo autor.

Cartões com chip microprocessador

Uma arquitetura típica deste tipo de cartões é apresentada na Figura 2.4 (b). Cartões com chip de microprocessador têm o escopo para satisfazer os requisitos de um cartão inteligente, pois, eles não apenas armazenam e comunicam valores armazenados, mas podem fazê-lo dentro do contexto de programas de protocolo de segurança. A *interface* do protocolo para o dispositivo pode ser definida de tal forma que é logicamente impossível extrair informações ou reprogramar o conteúdo sem permissões apropriadas que são verificadas e aplicadas pela funcionalidade criptográfica. À primeira vista, alguém poderia pensar que a busca acabou e que a presença de um cartão com chip microprocessador é sinônimo de um cartão inteligente, mas este não é o caso.

Um cartão de microprocessador convencional não especializado pode fornecer segurança lógica, mas isso é insuficiente para um cartão inteligente. Os invasores não são impedidos pela segurança lógica, mas empregam uma variedade de técnicas que atacam o chip diretamente ou exploram o vazamento de informações de um dispositivo operacional. Esses ataques são descritos em detalhes dentro do item 2.1.5, mas basta dizer que um microprocessador usado em um cartão inteligente é projetado de uma maneira muito especializada para ser **resistente a violações** (ANDERSON; KUHN, 1996). Então, um cartão inteligente contém um chip microprocessador inviolável (incorporando contramedidas contra-ataques conhecidos) que é difícil forjar ou copiar. Ele inclui um ID exclusivo, pode participar de transações eletrônicas automatizadas, armazenar dados com segurança e executar/hospedar uma série de protocolos e algoritmos de segurança.

2.1.2 Características do cartão inteligente

Até agora, uma substancial abordagem foi dada a cartões inteligentes; no entanto, como qualquer dispositivo, eles têm pontos fortes e fracos. Para explorar apropriadamente é tão importante apreciar os pontos fracos quanto os pontos fortes, ver a Tabela 2.1, onde se apresenta um resumo sucinto. Observe que as capacidades de memória e os recursos da CPU são apenas indicações típicas, à medida que evoluem com o tempo.

Tabela 2.1 – Resumo dos pontos fortes e fracos do cartão inteligente.

Características	**Limitações**
CPU (16–32 bit)	indefenso solo
RAM (4–16 kb)	sem fonte de alimentação interna
ROM/Flash (128–256 kb)	Restrições externas ao consumo de energia
EEPROM (64–256 kb)	Nenhuma interface de usuário
Opção de processador criptográfico	Sem relógio
Muito pequeno	Limitado (por comparação de PC)
Baixa potência	Memória
Baixo custo	Baixa velocidade do CPU
Seguro	Dispositivo implantado
Padronizado	Cartões legados podem ser inflexíveis
Sistemas operacionais	Novos cartões exigem implantação
Ferramentas de desenvolvimento	
Vários fornecedores	
Consistente e controlável	

Fonte: Adaptado de (MAYES; MARKANTONAKIS, 2017).

O fato de que o cartão está sem defesa por ser só é, portanto, sempre dependente de outros elementos do sistema. Por exemplo, um cartão inteligente convencional não tem fonte de energia interna, nenhuma interface direta com o usuário e (com poucas exceções) nem mesmo um relógio. Do ponto de vista de gerenciamento do sistema, outro recurso significativo é a capacidade de personalizar o cartão inteligente para um cliente ou conta em particular. Os cartões inteligentes tendem a ser emitidos em números muito grandes e, um dos problemas sempre presente é lidar com dispositivos legados. Um ótimo serviço de novos cartões recém emitidos pode levar anos para atingir uma grande proporção da base de clientes. Os problemas legados podem ser minimizados pelo design voltado para o futuro e pelo uso de sistemas de gerenciamento do ciclo de vida; no entanto, os problemas herdados costumam ser projetados para satisfazer as economias de custos de curto prazo.

2.1.3 Aplicações atuais de cartões inteligentes

Os cartões inteligentes são usados em diversos sistemas no mundo real, porém, são propostos para numerosas aplicações futuras. Na verdade, a capacidade e o número de cartões estão crescendo rapidamente em todas as áreas de uso. Algumas das aplicações mais notáveis estão em:

- Comunicações Móveis;
- Pagamento/Bancário;
- Transporte;
- Cartões de identidade do governo/passaportes;
- Cartões de Titularidade/Cartões de Saúde;
- Controle de Acesso Físico;
- Controle de acesso de TI;
- TV via satélite.

Para as comunicações móveis, o foco tem sido nos cartões SIM (*subscriber identity module*); no entanto, um *smartphone* com capacidade NFC (*Near Field Communication*) pode incorporar um elemento de segurança (*Secure Element* - SE) de hardware. O SE embutido (eSE) é muito parecido com um chip de cartão inteligente resistente a ataques que pode ser encontrado em um SIM, e a sua presença pode eventualmente desafiar a exigência de um cartão SIM de operador removível. Os computadores e talvez os telefones também podem incluir um Módulo de plataforma confiável (*Trusted Platform Module*-TPM), projetado para fornecer garantia no estado correto da plataforma e do software de computação. O chip TPM tem um papel muito específico e, não é tão flexível quanto um chip de cartão inteligente; no entanto, as propriedades resistentes a ataques são muito semelhantes.

A Figura 2.5, mostra uma estimativa (fonte original Infineon 2014) para o mercado anual de chips microcontroladores, incluindo aplicativos de cartões inteligentes e uso incorporado. O volume total do mercado é enorme e continua crescendo, e previa-se que subisse ate aproximadamente de 9 bilhões em 2013 para em torno de 13 bilhões em 2018. Esses números são ainda mais notáveis quando se percebe que eles não incluem os tipos mais simples de RFID e que as previsões não atenderam à demanda potencial devido ao impulso em direção à Internet das Coisas (IoT).

No gráfico, ilustra-se que as comunicações móveis ainda dominam o mercado na forma do cartão GSM (STÜBER, 2017) SIM e do cartão USIM equivalente a 3G/UMTS (HILLEBRAND, 2002) (usamos o termo SIM para nos referir a ambos). Embora sempre haja discussão sobre os cartões SIM serem abandonados por chips incorporados, isso ainda não aconteceu em grande escala, e as Operadoras de Rede Móvel (MNO) estão resistindo à mudança. Até o momento, existem mais de 4,5 bilhões de assinantes de telefonia móvel

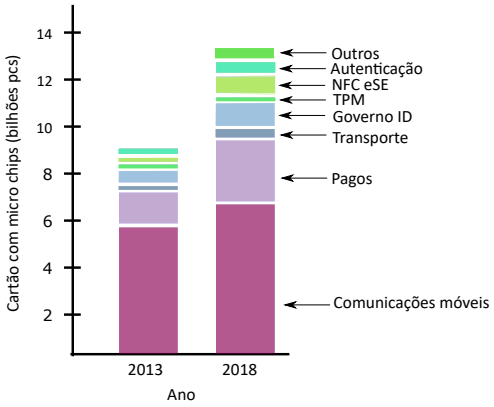


Figura 2.5 – Mercado anual de chips microcontroladores nos cartões inteligentes.

Fonte: Adaptado de fonte original Infineon 2014.

e, como os SIMs se tornaram itens descartáveis, não surpreende que cerca de 6 bilhões de SIMs estejam sendo emitidos a cada ano. Apesar da sua onipresença e de reduzir a vida útil, os SIMs tendem a estar entre os cartões tecnicamente mais avançados em uso, o que contrasta com os cartões telefônicos de crédito de chamada muito simples que apareceram pela primeira vez nas redes de telefonia fixa. Após as comunicações, o pagamento ainda está em segundo lugar e os seus volumes cresceram conforme o padrão EMV de chip e PIN ganhou impulso em todo o mundo. Os 3 bilhões estimados para 2018 podem até ser subestimados, considerando que o EMV está agora se estabelecendo nos EUA.

2.1.4 Segurança de cartão inteligente

Um dos principais motivos pelos quais os cartões inteligentes existem é a segurança, o próprio cartão fornece uma plataforma computacional na qual as informações podem ser armazenadas com segurança e as operações podem ser executadas de forma segura. Nos sistemas financeiros, informações confidenciais, como números de contas bancárias, podem ser armazenadas num cartão inteligente. Em aplicações de bolsa eletrônica (cartões de dinheiro e similares), o desequilíbrio de alguma moeda negociável pode ser armazenado em um cartão esta moeda pode ser creditada ou debitada por terminais externos (sistemas) em uma transação local. Em sistemas de acesso físico (por exemplo, abrir a porta do escritório), um cartão inteligente pode conter a chave pela qual um sistema eletrônico pode ser atraído para destravar a porta e permitir a entrada. Em sistemas de rede ou mesmo em sistemas de computadores locais, o cartão inteligente pode conter a senha pela qual um usuário é identificado na rede ou no sistema local e através do qual os privilégios são concedidos por esses sistemas para acessar informações ou processar recursos.

Todos estes sistemas aparentemente desconexos têm necessidades e características operacionais muito semelhantes, particularmente no que diz respeito à segurança desses

sistemas. Com base nisso, vamos examinar alguns dos sistemas de características gerais que coletivamente são chamados de segurança. O termo **segurança** é frequentemente usado para se referir a uma variedade de características relacionadas à realização de transações entre duas ou mais partes de tal maneira que qualquer pessoa envolvida na transação confie na integridade e, talvez, na privacidade da transação.

2.1.5 Tipo de ataques em cartões inteligentes

Nesta seção, para avaliação de segurança, Vamos nos concentrar em ataques voltados à recuperação de algoritmos de segurança e material de criptografia armazenados em microcontroladores, cartões inteligentes e outros processadores de segurança no nível de chips.

Podemos distinguir cinco principais categorias de ataque:

Microprobing estas técnicas podem ser usadas para acessar a superfície do chip diretamente, permitindo observar, manipular e interferir no CI.

Engenharia reversa é usado para entender a estrutura interna do chip semicondutor e aprender ou emular sua funcionalidade. Requer o uso da mesma tecnologia disponível para os fabricantes de semicondutores e dá capacidades semelhantes ao atacante.

Geração de falhas técnicas que usam condições ambientais anormais para gerar falhas no processador que fornecem acesso adicional.

Ataques de software usam a interface de comunicação normal do processador e exploram as vulnerabilidades de segurança encontradas nos protocolos, nos algoritmos criptográficos ou em sua implementação.

Ataques de canal lateral permitem que o atacante monitore, com alta resolução de tempo, as características analógicas das conexões de fornecimento e interface através do monitoramento de qualquer radiação eletromagnética emitida pelo processador durante a operação normal.

Todas as técnicas de *microprobing* e engenharia reversa são ataques invasivos. Eles exigem horas ou semanas em laboratório especializado e no processo eles destroem a embalagem. Os outros três são ataques não invasivos. O dispositivo atacado não é fisicamente danificado durante esses ataques. A última categoria de ataque também pode ser semi-invasiva. Isso significa que o acesso ao chip é necessário, mas o ataque não é penetrativo e a falha é gerada com pulso de luz de elevada intensidade, radiação, aquecimento local ou outros meios.

Os ataques não invasivos são particularmente perigosos em alguns aplicativos por dois motivos. Em primeiro lugar, o proprietário do dispositivo pode não perceber que as

chaves secretas ou os dados foram roubados, portanto, é improvável que a validade das chaves comprometidas seja revogada antes de serem violadas. Em segundo lugar, os ataques não invasivos geralmente se adaptam bem, já que o equipamento necessário geralmente pode ser reproduzido e atualizado a baixo custo.

O design da maioria dos ataques não invasivos requer conhecimento detalhado do processador e do software. Por outro lado, os ataques invasivos do tipo *microprobing* exigem muito pouco conhecimento inicial e geralmente trabalham com um conjunto similar de técnicas em uma ampla gama de produtos. Os ataques, portanto, geralmente começam com engenharia reversa invasiva, cujos resultados ajudam a desenvolver ataques não invasivos mais rápidos e mais baratos. Ataques semi-invasivos podem ser usados para aprender a funcionalidade do dispositivo e testar seus circuitos de segurança. Como esses ataques não exigem o estabelecimento de contato físico com as camadas internas de chip, não são necessários equipamentos caros, como cortadores a laser e máquinas de feixe de íons focalizado (*Focused Ion Beam* - FIB). O atacante poderia ter sucesso usando um simples microscópio de prateleira com um flash ou um apontador laser anexado a ele.

Os ataques podem ser reversíveis quando o dispositivo puder ser colocado de volta no estado inicial ou irreversível com alterações permanentes feitas no dispositivo. Por exemplo, a análise de potência e o micro revestimento podem dar ao atacante um resultado sem prejudicar o próprio dispositivo. Certamente, a técnica de *microprobing* irá deixar evidência de falsificação, mas geralmente isso não afeta a operação do dispositivo. Pelo contrário, a injeção de falhas e os ataques de luz UV poderiam muito provavelmente colocar o dispositivo no estado em que os registros internos ou o conteúdo da memória são alterados e não podem ser restaurados. Além disso, os ataques UV deixam evidência de violação, pois exigem acesso direto à superfície do chip.

Ataques Invasivos

São ataques que começam com a remoção do pacote do chip. Uma vez que o chip é aberto, é possível realizar ataques de sondagem ou modificação.Esse tipo de ataque pode, pelo menos em teoria, comprometer a segurança de qualquer microprocessador seguro. No entanto, esses ataques geralmente exigem equipamentos muito caros e um grande investimento em tempo para produzir resultados. A ferramenta mais importante para ataques invasivos é uma estação de trabalho com *microprobing*. Seu principal componente é um microscópio óptico especial com uma lente objetiva de longa distância de trabalho. Os microposicionadores são instalados em uma plataforma estável ao redor do soquete de teste de cavacos e permitem o movimento dos braços da sonda, com precisão submicrométrica, sobre uma superfície de chip. Uma agulha de sondagem com um fio elástico na extremidade é instalada em cada braço e permite o contato elétrico com as linhas de bus no chip sem danificá-las.

Um exemplo de tal ataque seria colocar sondas em linhas de bus entre blocos de um CI (um buraco precisa ser feito na camada de passivação do CI para permitir isso). Um invasor pode tentar obter informações secretas observando as informações enviadas de um bloco para outro.

Na sua forma mais extrema, esse tipo de ataque poderia usar um feixe de íons, destruir ou criar faixas na superfície do chip. Em teoria, isso poderia, ser usado para reconectar fusíveis. Tradicionalmente, os fabricantes de chips costumavam usar um modo de teste onde era possível ler e gravar em todos os endereços de memória enquanto um fusível estava presente. Uma vez que o fusível foi queimado dentro do chip (antes do chip sair da fábrica do fabricante), este modo não estava mais disponível. Nos microprocessadores seguros modernos, este circuito de teste é tipicamente removido quando o chip é cortado da matriz, evitando o ataque. Mais informações sobre ataques invasivos estão disponíveis em (ANDERSON; KUHN, 1996; KÖMMERLING; KUHN, 1999). Mais recentemente, Tarnovsky (TARNOVSKY, 2008) fez vídeos sobre como esses ataques são conduzidos.

Ataques semi-invasivos

Ataques semi-invasivos, como ataques invasivos, exigem que a superfície do chip seja exposta. Mas a camada de passivação do chip permanece intacta (SKOROBOGATOV, 2005). Os métodos semi-invasivos não exigem contato elétrico com a superfície do metal, portanto, não há danos mecânicos ao silício. Porém, um invasor procura comprometer a segurança do microprocessador seguro sem modificar diretamente o chip. Os ataques semi-invasivos se tornam mais atraentes, pois não exigem ferramentas caras e dão resultados em menos tempo. Além disso, sendo aplicado a um transistor inteiro ou mesmo a um grupo de transistores, eles são menos críticos para o tamanho pequeno dos chips modernos.

Ataques semi-invasivos poderiam, em teoria, ser realizados usando ferramentas como luz UV, raios-X, lasers, campos eletromagnéticos e aquecimento local. Eles poderiam ser usados individualmente ou em conjunto uns com os outros. No entanto, este campo quase não foi explorado.

Ataques não invasivos

Este tipo de ataques buscam obter informações sem modificar um cartão inteligente, ou seja, tanto o microprocessador seguro quanto o cartão de plástico não são afetados. Um invasor tentará obter informações observando as informações filtradas durante a execução de um determinado comando ou tentando injetar falhas usando mecanismos diferentes por incidência de um feixe de luz. Os ataques não invasivos mais utilizados incluem brincar com a tensão de alimentação e o sinal do relógio. Ataques de subtensão e sobretensão podem ser usados para desabilitar o circuito de proteção ou forçar um processador a

realizar a operação incorreta. Além disso, se um protocolo de segurança for implementado incorretamente, isso deixará um buraco para o invasor explorar. Alguns microcontroladores e cartões inteligentes têm uma interface de teste de fábrica que fornece acesso à memória no chip e permite que o fabricante teste o dispositivo. Se um invasor puder encontrar uma maneira de explorar essa interface, ele poderá extrair facilmente as informações armazenadas no chip. Normalmente, informações sobre os circuitos de teste são mantidas em segredo pelo fabricante, mas um invasor pode tentar aplicar diferentes voltagens e níveis lógicos nos pinos, na esperança de colocá-lo no modo de teste. Isso às vezes funciona para microcontroladores, mas em cartões inteligentes esses circuitos de teste são geralmente destruídos após o uso.

Portanto, eles são considerados a ameaça mais séria à segurança de hardware de qualquer dispositivo. Geralmente é necessário muito tempo e esforço para encontrar um ataque em qualquer dispositivo específico. Isso geralmente envolve a engenharia reversa do dispositivo, no sentido de desmontar seu software ou entender seu layout de hardware. Alguns exemplos desse tipo de ataque seriam observar o consumo de energia de um microprocessador (KOCHER; JAFFE; JUN, 1999) ou injetar falhas ao colocar uma falha técnica na fonte de alimentação (ANDERSON; KUHN, 1996).

2.2 Sensores de temperatura

Um sensor de temperatura é um circuito ou dispositivo que produz uma saída de tensão ou corrente conhecida ou específica de acordo com a variação de temperatura. Estes circuitos que variam com a temperatura monitoram a temperatura ambiente, e notificam as variações de temperatura. Se o circuito de detecção for mais inteligente, detectam quando um limite específico é excedido, tomando uma ação preventiva para diminuir a temperatura. Para medir essas variações existem quatro tipos de sensores de temperatura comumente usados como mostra a Tabela 2.2, com suas comparações de propriedades comuns entre termopar, detector resistivo de temperatura (RTD) de platina, termistor e sensor BJT.

Tabela 2.2 – Comparação das propriedades de sensores de temperatura.

	Par termoelétrico	**RTD de Platina**	**Termistor**	**Sensor BJT**
Sensibilidade	0,02 mV/°F	0,21 mV/°F	2 mV/°F	$10 - 20$ mV/K
Faixa de Temp.	-320 to 2300 °F	-320 to 1200 °F	-150 to 300 °F	-55 to 150 °C
Estabilidade (por ano)	1 a 2 °F	±0,01% °F	±0,2 to ±0,5°F	-
Linearidade	Média	Boa	baixa	1 °C

Fonte: Adaptado de <www.transcat.com> & <www.analog.com>.

Estes sensores têm vantagens e desvantagens que podem ser observados na Figura 2.6. Considerando esses pontos, pode-se responder a seguinte pergunta: por que usar sensores CI no lugar de outras tecnologias como Termopares, RTDs e Termistores? Porque os sensores analógicos de estado sólido CI fornecem uma saída de tensão ou corrente que é proporcional à temperatura sem circuitos adicionais. Os sensores CI não requerem linearização ou outros circuitos. Além disso, o custo dos sensores CI também é muito competitivo, em alguns casos, menos caro do que sensores RTD e termistor.

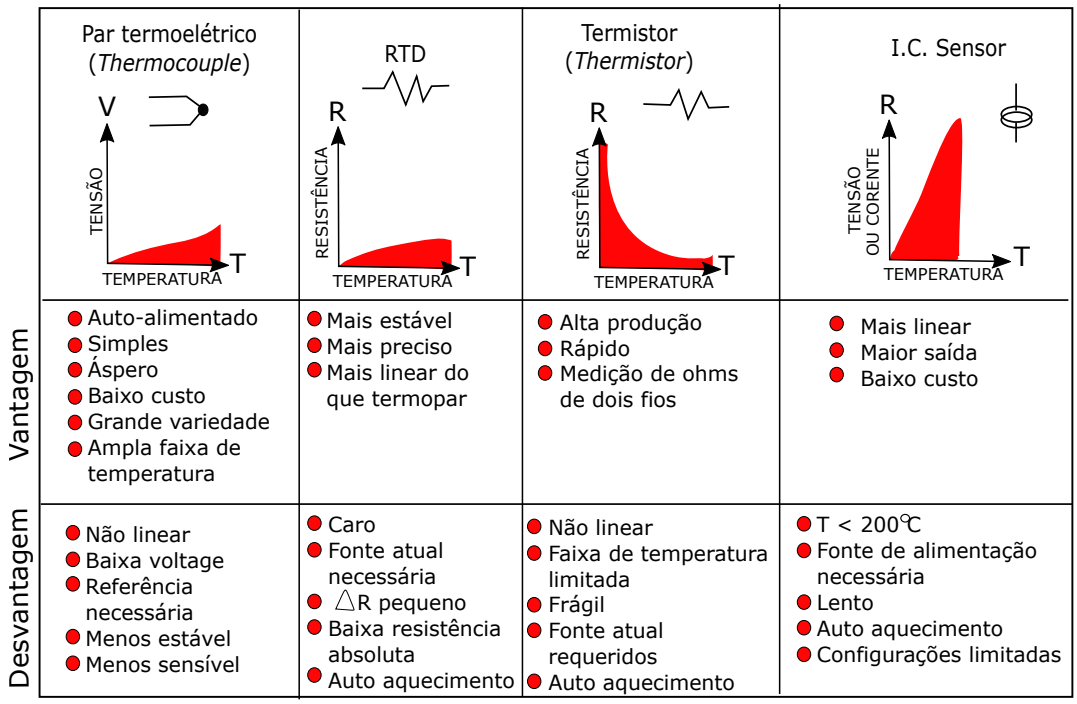


Figura 2.6 – Tipos de sensores de temperatura e suas vantagens e desvantagens.

Fonte: Adaptado de <https://sea.omega.com/ph/prodinfo/Integrated-Circuit-Sensors.html>.

Porém, os sensores de temperatura mais comumente implementados em CI são tais que a saída de tensão aumenta com a elevação da temperatura (que possua derivada positiva) é conhecida como PTAT (*Proporcional To Absolute Temperature*), enquanto outra que reduza com a elevação da temperatura (que possua derivada negativa) é conhecida como CTAT (*Complementary to Absolute Temperature*).

2.2.1 Tecnologia CMOS

As características importantes do modelo, como mobilidade, tensão limite, velocidade de saturação, resistência de séries parasitárias e características das junções fonte/dreno, de um dispositivo CMOS são dependentes da temperatura (CHENG; HU, 1999). Isso torna vulneráveis ao acesso a informação de circuitos que empregam esses dispositivos. Para

evitar essa vulnerabilidade de acesso é necessário desenvolver sensores de temperatura e emprega-los na proteção de CI na tecnologia CMOS.

Nos sensores, propriamente ditos, deve-se evitar o uso de transistores CMOS, por exemplo, uma vez que a tenção o corrente fornecida pelo sensor, como indicação da temperatura dependerá não somente destas variações mas de outros fatores inerentes ao sensor. Isso resultaria em imprecisão da medida. Por outro lado, transistores bipolares apresentam menor sensibilidade aos fatores que tem o transistor CMOS, porem sendo melhor na medição de temperatura. Diversas arquiteturas são possíveis para esses sensores. Arquiteturas que produzem tensão em função da temperatura são apresentados a seguir.

Transistor de junção bipolar (BJT)

Para criar um sensor de temperatura preciso, é absolutamente essencial a necessidade de um elemento que tenham um comportamento linear com a variação de temperatura. Esse elemento deve ser altamente tolerante a variações de processo e também apresentar alta repetibilidade em sua saída.

Na tecnologia CMOS, as difusões normalmente usados para realizar MOSFETs, podem ser usadas também para criar transistores de junções bipolares (BJTs) como se mostra na Figura 2.7. Atualmente os transistores PNP verticais são preferidos devido à sua menor sensibilidade à dispersão do processo e precisão de empacotamento (PERTIJS; MEIJER; HUIJSING, 2004). Os PNPs geralmente oferecem flexibilidade na implementação, sendo o coletor é formado dentro do substrato P, portanto, não é diretamente accessível.

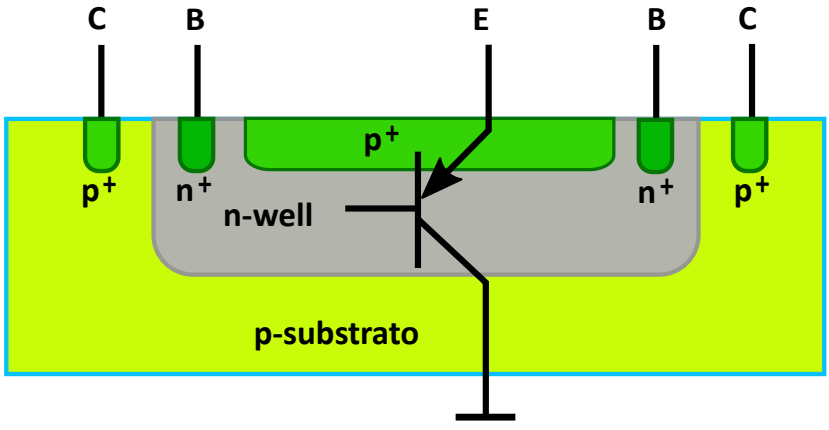


Figura 2.7 – Substrato PNP na tecnologia CMOS de poço n-well.

Fonte: Adaptado de Pertijs.

Para aproveitar a junção PN de um transistor bipolar, sua base pode ser conectada ao coletor, resultando em um dispositivo de dois terminais formado pelo emissor e pela

base/coletor. O comportamento do transistor será, então, muito semelhante a um diodo (junção PN) como mostra na Figura 2.8.

2.2.2 Tensão com coeficiente térmico negativo (CTAT)

Para as arquiteturas ilustradas na Figura 2.8 o coeficiente térmico da tensão fornecida é negativo, sendo elas denominadas arquiteturas CTAT (*Complementary to Absolute Temperature*). A tensão fornecida é a tensão V_{BE} no caso de um transistor NPN, V_{EB} no caso de um transistor PNP e V_D no caso de um diodo.

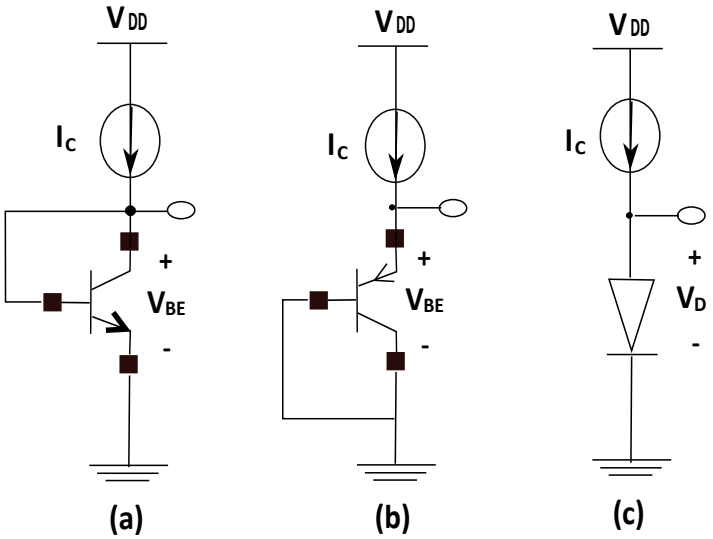


Figura 2.8 – Forma de obter uma tensão CTAT. (a) Utilizando transistor NPN. (b) Utilizando transistor PNP. (c) Transistores estão conectados como Diodo.

Fonte: Adaptado de Razavi,B.

As equações para os dois tipos de transistores são as mesmas, bastando trocar V_{BE} por V_{EB} para utilizar o transistor PNP. Sejam, I_C a corrente do coletor, I_S a corrente de saturação do transistor bipolar e V_T a tensão térmica. Para um dispositivo bipolar pode-se escrever que:

$$I_C = I_S.e^{V_{BE}/V_T} \tag{2.1}$$

Onde $V_T = kT/q$ sendo k a constante de Boltzmann, T a temperatura e q a carga do elétron.

A corrente de saturação I_S é proporcional a μkTn_1^2, onde μ denota a mobilidade dos portadores minoritários e n_1 é a concentração de portadores minoritários no silício. A dependência destas grandezas com a temperatura é representada como $\mu \propto \mu_0 T^m$ onde $m \approx -3/2$ e ${n_i}^2 \propto T^3 * e^{[-E_g/(kT)]}$ onde $E_g \approx 1,12eV$ é a energia de *band-gap* do silício.

Assim,

$$I_s = bT^{4+m}e^{-\frac{E_g}{kT}} \tag{2.2}$$

Onde b é o fator de proporcionalidade. Escrevendo $V_{BE} = V_T ln(I_C/I_S)$, pode-se calcular o coeficiente térmico da tensão base-emissor (V_{BE}) do transistor bipolar. Derivando em relação à temperatura (T), é obtido o comportamento da corrente do coletor (I_C) com a temperatura. Para uma análise simplificada, assume-se por agora que I_C é mantida constante.

$$\frac{\partial V_{BE}}{\partial T} = \frac{\partial V_T}{\partial T} ln(\frac{I_C}{I_S}) - \frac{V_T}{I_S}\frac{\partial I_S}{\partial T} \tag{2.3}$$

Da equação (2.2), se obtêm:

$$\frac{\partial I_S}{\partial T} = b(4+m)T^{3+m}e^{\frac{-E_g}{kT}} + bT^{4+m}(e^{\frac{-E_g}{kT}})(\frac{E_g}{kT^2}) \tag{2.4}$$

E, portanto, com o auxilio de (2.2) pode-se concluir que:

$$\frac{V_T}{I_S}\frac{\partial I_S}{\partial T} = (4+m)\frac{V_T}{T} + \frac{E_g}{kT^2}V_T \tag{2.5}$$

com a ajuda da equação (2.3) e (2.5), pode-se escrever que a equação (2.3) conduz a,

$$\frac{\partial V_{BE}}{\partial T} = \frac{V_T}{T} ln\frac{I_C}{I_S} - (4+m)\frac{V_T}{T} - \frac{E_g}{kT^2}V_T \tag{2.6}$$

E assim:

$$\frac{\partial V_{BE}}{\partial T} = \frac{V_{BE} - (4+m)V_T - E_g/q}{T} \tag{2.7}$$

Por meio da equação (2.7) se obtém o coeficiente de temperatura da tensão base-emissor em uma dada temperatura. Também foi revelada uma dependência sobre a magnitude de seu próprio V_{BE}.

2.2.3 Tensão com coeficiente térmico positivo (PTAT)

Para a arquitetura ilustrada na Figura 2.9 o coeficiente térmico da tensão fornecida é positivo, sendo ela denominada arquitetura PTAT (*Proporcional To Absolute Temperature*). A tensão fornecida é a diferença entre as tensões base-emissor de dois transistores bipolares operando com correntes diferentes. Por exemplo, se dois transistores idênticos ($I_{S1} = I_{S2}$) polarizados com correntes de coletor iguais a nI_0 e I_0, desprezando a corrente de base.

Tem-se que:

$$\Delta V_{BE} = V_{BE1} - V_{BE2} \tag{2.8}$$

$$\Delta V_{BE} = V_T ln\frac{nI_0}{I_{S1}} - V_T ln\frac{I_0}{I_{S2}} \tag{2.9}$$

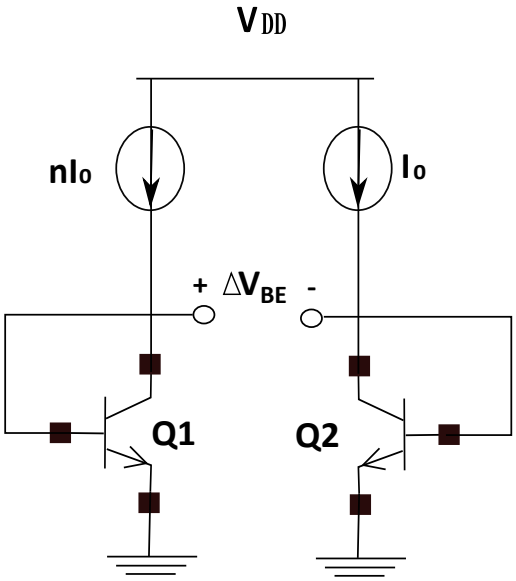


Figura 2.9 – Forma de obter uma tensão PTAT, utilizando dois transistores NPN.

Fonte: Adaptado de (RAZAVI, 2016).

$$\Delta V_{BE} = V_T ln n \tag{2.10}$$

Assim, a diferença V_{BE} exibe um coeficiente de temperatura positivo:

$$\frac{\partial \Delta V_{BE}}{\partial T} = \frac{k}{q} ln n \tag{2.11}$$

2.2.4 Circuito de referências de *band-gap*

O circuito de referência de *band-gap* começou em 1971, por Robert Widlar que introduziu um circuito simples para implementar uma tensão de referência que varia pouco em uma ampla faixa de temperatura (WIDLAR, 1970). Este circuito é mostrado na Figura 2.10, que usa três transistores de junção bipolar (BJTs) para implementar os componentes PTAT e CTAT. O componente PTAT vem de Q1 e Q2. Escrevendo a Lei de Voltagem de Kirchhoff (KVL-*Kirchhoff's Voltage Law*) em torno de Q1, Q2 e R3, verifica-se que a voltagem através de R3 é:

$$V_{R3} = V_{BE1} - V_{BE2} = \Delta V_{BE} \tag{2.12}$$

Assumindo um grande ganho de corrente para Q2, o que implica $\beta >> 1$, então a tensão em R2 é:

$$V_{R2} = \frac{\Delta V_{BE}}{R_3} * R_2 \tag{2.13}$$

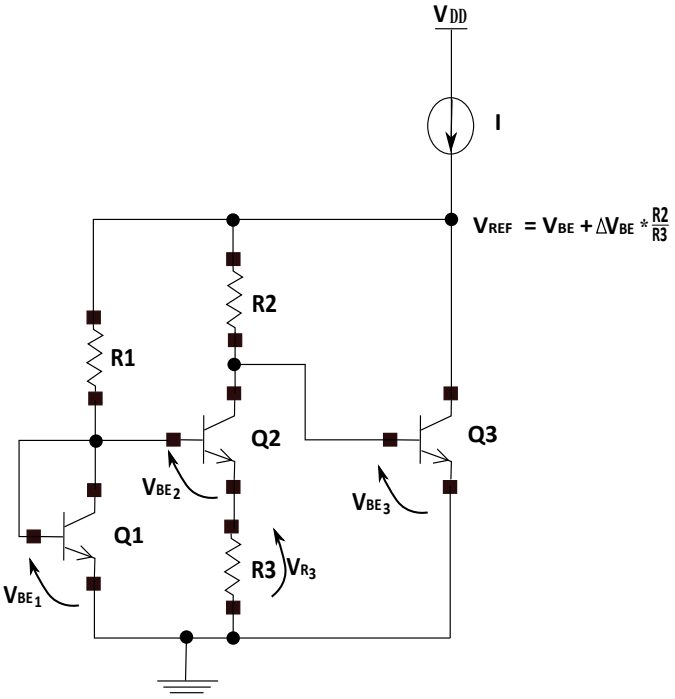


Figura 2.10 – Diagrama de circuito simples de referência *band-gap* original.

Fonte: Adaptada de (*Widlar's band-gap circuit*).

Em seguida, um adicional a KVL é escrito considerando Q3, R2 e a tensão de saída, VREF. Esta equação mostra:

$$V_{REF} = V_{BE} + \Delta V_{BE} * \frac{R_2}{R_3} \tag{2.14}$$

Além disso, a diferença das tensões base-emissor pode ser escrita em termos de suas densidades de corrente, expressas como J1 e J2. A densidade de corrente é a razão entre a corrente do coletor e a corrente de saturação reversa do BJT.

$$\Delta V_{BE} = \frac{KT}{q} * \ln(\frac{J1}{J2}) \tag{2.15}$$

Observando apenas os componentes variáveis da temperatura do V_{REF}, sua equação se torna.

$$V_{REF} = V_{BE} + \frac{KT}{q} * \ln(\frac{J1}{J2}) = V_{g0}(1 - \frac{T}{T_0}) + V_{BE0}(\frac{T}{T_0}) + \frac{KT}{q} * \ln(\frac{J1}{J2}) \tag{2.16}$$

Os resistores $R2$ e $R3$ não são incluídos porque seus coeficientes de temperatura se cancelam. Em última análise, é mostrado que, ao definir a derivada de V_{REF} em relação

a uma temperatura igual a zero, a saída será totalmente compensada pela temperatura fornecida.

$$V_{g0} = V_{BE0} + \frac{KT}{q} * \ln(\frac{J1}{J2}) \tag{2.17}$$

Desde que a soma da tensão inicial emissor-base e do termo PTAT seja igual à tensão *band-gap* do silício a 0 K, a tensão de referência fornecida será estável ao longo da temperatura. Na prática, devido aos maiores efeitos de ordem não considerados na derivação, a tensão de saída será levemente maior que 1,205 V (WIDLAR, 1971).

Em termos de valores reais, uma variação típica de temperatura de um VBE é de $-1,5mV/K$ à temperatura ambiente (RAZAVI, 2016). Isso significa que a porção PTAT deve ter um coeficiente de temperatura de $+1,5mV/K$. Para que isso seja alcançado, então $KT/q * ln(J1/J2)$, que pode ser re-expresso em unidades de mV/K como $0,087 * ln(J1/J2)mV/K$, precisa ser $+1,5mV/K$. Para que isso ocorra, a taxa de densidade de corrente precisaria ser $3,07 * 10^7$. Como a densidade de corrente é proveniente de correntes de escala e dimensionamento de dispositivos, é muito pouco prático obter esse tipo de razão de densidade de corrente em um CI. Isso mostra a necessidade de ter um fator de escala para a tensão PTAT, de modo que a taxa de densidade de corrente possa ser reduzida.

2.2.5 Circuito original de *band-gap* CMOS

Neste circuito, a saída final é muito semelhante ao circuito original de Widlar, embora o circuito seja bem diferente. Este circuito é mostrado na Figura 2.11, (NEUTEBOOM; KUP; JANSSENS, 1997).

Os bipolares neste design são dispositivos pnp e não há dependência de beta para este circuito, pois os dispositivos pnp são verticais e não compartilham a corrente. A chave deste design é o amplificador operacional que é usado para forçar os nós X e Y a serem equivalentes, de modo que ΔV_{BE} possa ser detectado através do resistor $R2$. Assumindo um amplificador operacional ideal, com ganho infinito e sem erros de offset, a tensão de saída pode ser encontrada via lei de KVL , onde V_{R2} e V_{R1} são voltagens em $R2$ e $R1$, respectivamente (SCHAEFFER et al., 2017).

$$V_{out} = V_{BE2} + V_{R2} + V_{R1} \tag{2.18}$$

Reconhecendo que o amplificador operacional fará com que a tensão no nó Y seja igual a V_{BE1}, ele é encontrado.

$$V_{out} = V_{BE2} + \Delta V_{BE} + \Delta V_{BE}\frac{R1}{R2} = V_{BE2} + \Delta V_{BE}(1 - \frac{R1}{R2}) \tag{2.19}$$

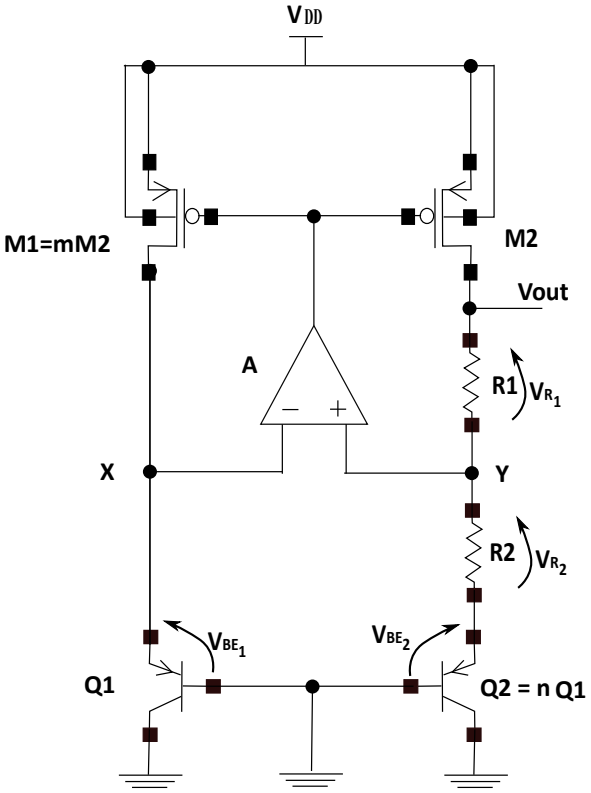


Figura 2.11 – Circuito de referencia de *band-gap* CMOS.

Fonte: Adaptado de (SCHAEFFER et al., 2017).

Esta expressão vem do fato de que a corrente através de $M2$ e $Q2$ é $\Delta V_{BE}/R2$. Se $Q2$ é n vezes $Q1$ e, em seguida, $M1$ é m vezes $M2$, então, mais uma vez, podemos escrever isso.

$$\Delta V_{BE} = \frac{KT}{q} \ln(m * n) \tag{2.20}$$

substituindo de equação (2.20) em equação (2.19) tem se,

$$V_{out} = V_{BE2} + \frac{KT}{q} \ln(m * n)(1 - \frac{R1}{R2}) \tag{2.21}$$

Isto é o mesmo que o circuito *band-gap* original, exceto por um fator adicional de adicionar 1 à relação de resistor R1/R2. Uma vantagem deste circuito é que ele requer apenas dois BJTs ao invés dos três BJTs requeridos pelo circuito *band-gap* original introduzido pela Widlar.

2.2.6 Sensor de temperatura na tecnologia CMOS

Atualmente a maioria dos circuitos sensores de temperatura na tecnologia CMOS, são desenvolvidos utilizando transistores bipolares como componentes básicos e comparadores (PERTIJS; MEIJER; HUIJSING, 2004). Pois a junção V_{BE} dos transistores bipolares

sofrem grande variação com a alteração da temperatura e os comparadores possuem uma alta velocidade de resposta.

Na Figura 2.12 é ilustrado um circuito de detecção térmica convencional que é muito utilizado (UENO et al., 2006; DENG et al., 2015). Onde a junção V_{BE} do transistor $Q1$ é responsável por sensibilizar a alteração da temperatura neste tipo de topologia. Como é notado, quando ocorre uma variação da temperatura também ocorre uma variação de tensão V_{BE}, do transistores bipolares. Partindo do ponto no qual o comportamento da variação de V_{BE}, na temperatura desejada, é projetado $R1$ e $R2$ para que quando atingir-se a temperatura desejada, ocorra a comutação na saída do comparador. O transistor $M1$ é responsável por gerar uma histerese necessária para o comparador.

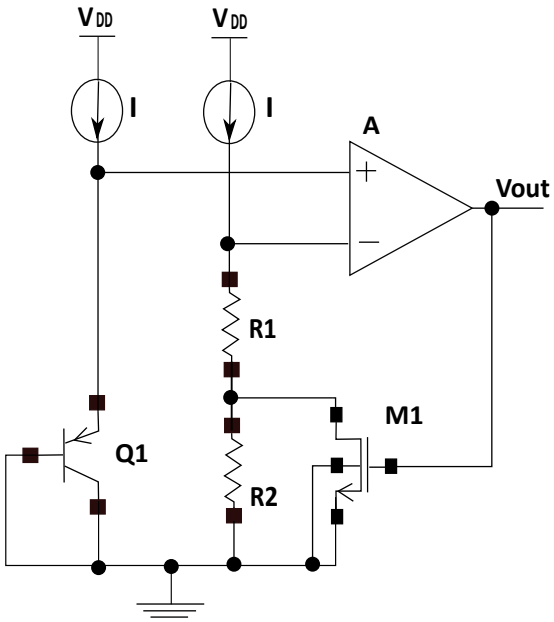


Figura 2.12 – Circuito de proteção térmica convencional.

Fonte: Adaptado de (BIN; QUAN-YUAN, 2009).

Esta topologia, dependendo da variação de V_{BE} e do tempo de resposta do comparador, pode ser aplicada na detecção de altas temperaturas apresentando uma boa estabilidade, mas apresentando duas desvantagens (BIN; QUAN-YUAN, 2009). A Primeira é que a corrente fornecida na malha de $Q1$ não é suficiente para manter a estabilidade do circuito, para diferentes tensões de alimentação. A segunda, por se tratar de dispositivo bipolar haverá também dissipação de potência por esse componente, e consequentemente todo o subtrato onde foi desenvolvido o CI irá se "beneficiar" desse indesejado aquecimento.

3 ARQUITETURA DE SENSOR DE TEMPERATURA E RESISTÊNCIA A ADULTERAÇÃO

Este capítulo descreve o desenvolvimento de blocos do sistema de proteção de CI de cartão inteligente para proteção em temperatura e proteção contra adulteração. Para mais detalhes, o diagrama de blocos é apresentado na Figura 3.1. De acordo com este diagrama, inicialmente um sensor de temperatura CMOS é projetado com um número mínimo de transistores, dois comparadores de par diferencial de histerese (NMOS e PMOS) para controle de limites de temperatura pré-estabelecido e uma arquitetura de controle lógico. Na parte de proteção contra adulteração, um circuito com resistência variável é projetado e um comparador. O bloco total é projetado com baixo consumo de energia, pequena área para ser integrável no CI do cartão inteligente.

Diagrama de blocos proposto para o sensor.

Um circuito *bandgap* (CMOS) fornece a um circuito sensor (Temperatura & Resistivo) uma corrente de referência Iref, ao bloco comparadores, duas tensões de referência Vref1 e Vref2, uma para cada limite de temperatura pré-estabelecido. O sensor completo inclui, além disso, três comparadores (um para o resistor de adulteração) e um circuito de controle lógico, como mostrado na Figura 3.1.

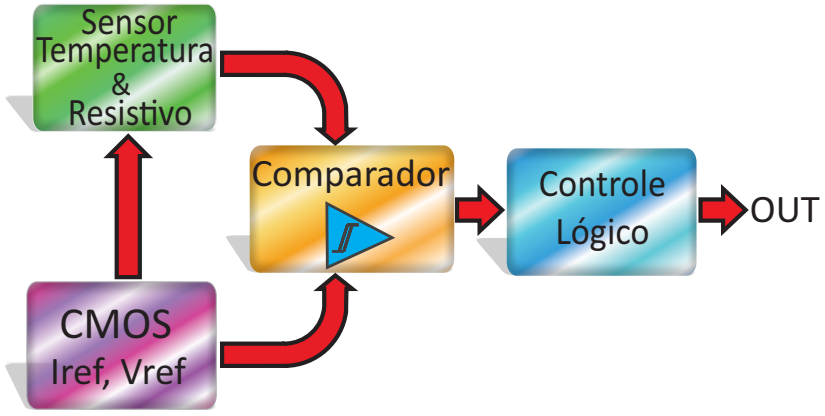


Figura 3.1 – Diagrama de blocos para proteção térmica e contra adulteração.

Fonte: Elaborado pelo autor.

3.1 Arquitetura de geração de tensão do sensor CTAT

O sensor de temperatura projetado nesta pesquisa é uma nova arquitetura proposta, a fim de atingir baixas e altas temperaturas, com baixa potência e uma quantidade mínima de transistores, em uma pequena área no layout. Nesta aplicação, além do uso de um bloco CTAT, é implementado com dois transistores MOS e apenas um transistor bipolar PNP. O circuito proposto é mostrado na Figura 3.2.

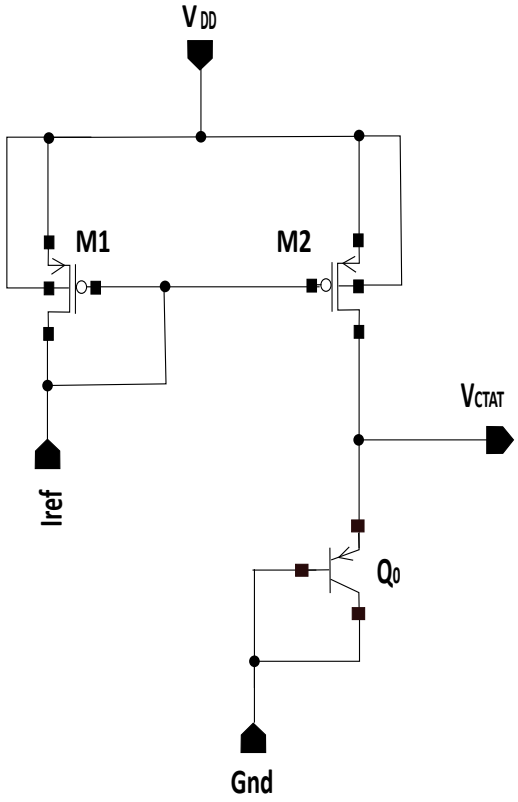


Figura 3.2 – Arquitetura do sensor de temperatura projetado para geração de tensão CTAT.

Fonte: Projetado pelo autor.

A maneira mais direta de usar um transistor bipolar como sensor de temperatura é usar sua tensão base-emissor V_{BE} como medida de temperatura (PERTIJS; MEIJER; HUIJSING, 2004). Se o transistor for polarizado em sua região ativa direta, a relação entre sua corrente de coletor I_C e sua tensão base-emissor V_{BE} é dada pela equação 2.1,encontrada na seção 2.2.2. A partir desta equação exponencial bem conhecida; a seguinte expressão para V_{BE} em função da temperatura absoluta T pode ser dada como(equação 3.1).

$$V_{BE}(T) = V_{g0}(1 - \frac{T}{T_r}) + \frac{T}{T_r}V_{BE}(T_r) - \eta\frac{kT}{q}ln(\frac{T}{T_r}) + \frac{kT}{q}ln(\frac{T}{T_r}) \tag{3.1}$$

Onde: V_{g0} é a tensão de *band gap* extrapolada em $0K$ ver equação 2.17, η é uma

constante dependente do processo; K é a constante de Boltzmann; q é a carga do elétron; e T_r é uma temperatura de referência arbitrária. $V_{BE}(T)$ é uma função quase linear da temperatura 2.7, com uma inclinação típica de $2mV/K$. A não linearidade, ou curvatura, é representada pelos dois últimos termos da equação 3.1.

As diferentes especificações para o sensor de temperatura são dadas principalmente pelos blocos que estão conectados a ele. Neste caso, o intervalo de temperatura e as especificações de erro variam do CI. A calibração deve ser realizada usando uma temperatura controlada através da medição da tensão de saída do sensor (CTAT) e, em seguida, usando a inclinação média, calculamos a nova função da tensão de saída, mostrada na Figura 3.3 para atingir o objetivo.

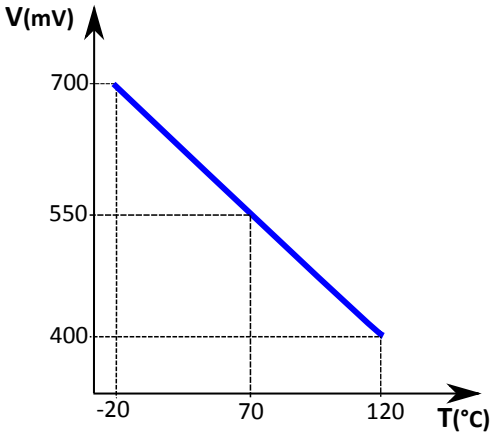


Figura 3.3 – Tensão CTAT em função da temperatura.

Fonte: Elaborado pelo autor.

Para atingir nosso objetivo a equação da reta, mostra um coeficiente angular (pendente) de $\frac{\partial V_{BE}}{\partial T} = -2,14mV/°\text{C}$. Comparado com o que foi deduzido nos capitulo 2 para variação de tensão com coeficiente término negativo (CTAT) a equação (2.7) leva para una inclinação típica de $2mV/K$. Mas na equação 2.7 podemos observar uma dependência sobre a magnitude de seu próprio V_{BE}, o qual é ajustado com a dimensão do transistor para variar a corrente de I_S e obter a inclinação desejada.

3.2 Comparador e controle lógico

3.2.1 Comparador de tensão diferencial com arquitetura de histerese

Os comparadores de tensão são componentes essenciais do sistema eletrônico. Comparadores com histerese são vantajosos em comparação com aqueles sem histerese quando usados em aplicações onde as entradas dos comparadores contém distorções de alta frequência, como

mostrado na Figura. 3.4. Os comparadores com histerese também são chamados *Schmitt trigger* (SMITH, 1988).

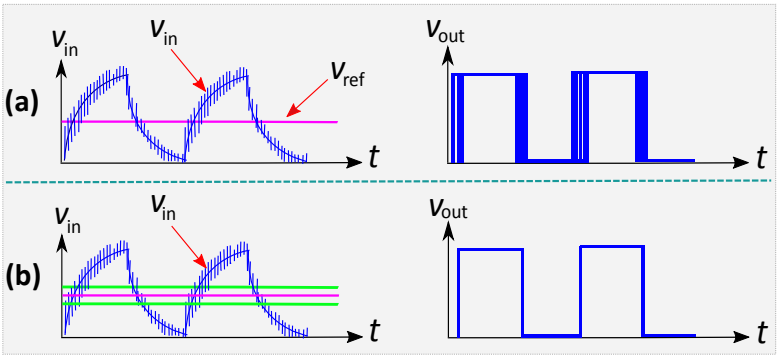


Figura 3.4 – Desempenho de comparadores (a) sem histerese e (b) com histerese.

Fonte: adaptado de Allen (ALLEN; HOLBERG, 2012).

Uma pequena quantidade de histerese pode ser útil em um circuito comparador porque reduz a sensibilidade do circuito ao ruído e ajuda a reduzir transições múltiplas na saída ao mudar o estado (SAXENA; SHRIVASTAVA; AKASHE, 2016). A curva de transferência completa do circuito é mostrada na Figura. 3.5

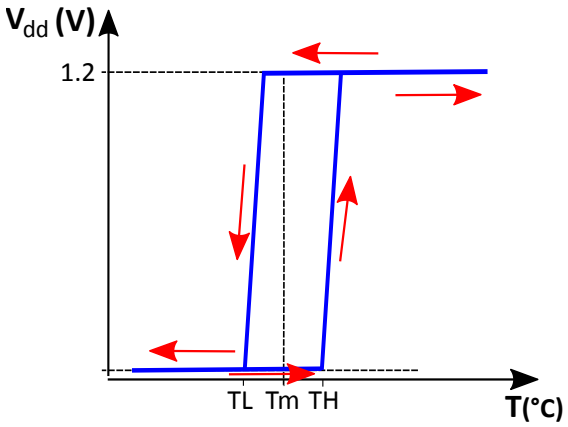


Figura 3.5 – Curva característica de histerese do comparador.

Fonte: Elaborado pelo autor.

O comparador projetado tem arquitetura proposta por Allstot (ALLSTOT, 1982). A esta especificação proposta é implementada com a configuração par diferencial NMOS e PMOS. A arquitetura do comparador completo com histerese interna de par diferencial PMOS é baseada no trabalho reportado por (ALLEN; HOLBERG, 2012) e que esta ilustrada na Figura. 3.6. Este comparador foi projetado para $V_{in+} = V_{ref1} = 400\,\text{mV}$, $I_{ref1} = I_{ref2} = 1\,\mu\text{A}$ e $V_{dd} = 1{,}2\,\text{V}$, da mesma forma para par diferencial NMOS $V_{in+} = V_{ref2} = 700\,\text{mV}$.

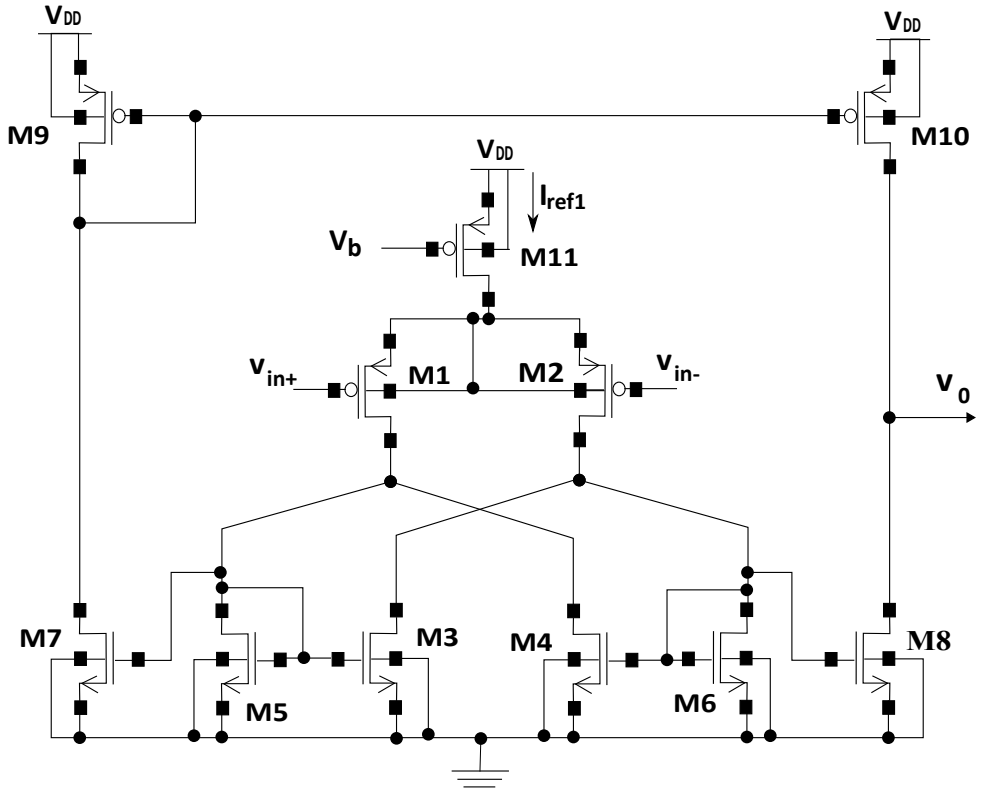


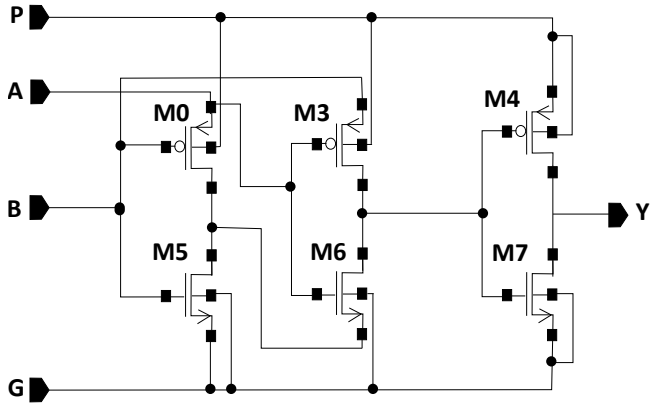
Figura 3.6 – Esquema dos comparador par diferencial PMOS.

Fonte: Adaptado de ALLEN.

3.2.2 Arquitetura de controle lógico

Os circuitos lógicos XOR e XNOR (exclusive-NOR) são as unidades fundamentais em diversos circuitos, como comparador, verificador de paridade, somador total e assim por diante. Se estas funções forem implementadas no nível da porta lógica, por porta elementar, AND, OR e NOT, a redução será muito grande (WANG; FANG; FENG, 1994). Na implementação do circuito XOR e XNOR em CMOS, é bastante conhecida que o transistor NMOS pode transmitir o sinal LOW (ou "0"), e o transistor PMOS pode transmitir um sinal HIGH (ou "1").

Com base nessa teoria e o circuito XOR de 4T (ANJALI; RAO, 2016), foi projetado o circuito logico da Figura. 3.7 que mostra o circuito funcional da porta lógica XNOR com 6 transistores, quando $A = B = 0$, temos um sinal alto na saída. Quando A = 0 e B = 1, temos um sinal baixo na saída; Quando A = 1 e B = 0, temos um sinal baixo na saída; E quando A = 1 e B = 1, temos um alto na saída.



XNOR

A	B	Y	M0	M5	M3	M6	M4	M7
0	0	1	S	C	S	C	S	C
0	1	0	C	S	S	C	C	S
1	0	0	S	C	C	S	S	C
0	0	1	C	S	C	S	S	C

Figura 3.7 – Diagrama de circuitos XNOR implementado a base de 6 transistores.

Fonte: Projetado pelo autor, baseada em XOR de 4T.

3.3 Resistência a adulteração

Os ataques invasivos ou semi-invasivos exigem a remoção de camadas de metal ou, pelo menos, a decapsulação da embalagem do chip, essas decapsulações são usadas para acessar as diferentes camadas existentes dos CIs. O simples acesso à superfície da matriz e a observação da estrutura do chip após a remoção das camadas de metal são os primeiros obstáculos para conduzir um ataque. A camada de metal dos cartões inteligentes não é uma proteção absoluta, porque os ataques invasivos começam com a remoção do encapsulamento do chip. Aquecer o plástico do cartão para amolecer a cola permite que o módulo do chip seja facilmente removido simplesmente dobrando o cartão. A matriz de silicone pode ser removida imergindo-se a ácido nítrico fumegante como mostra a Figura 3.8 e aquecendo em torno de 60 °C para dissolver completamente a resina de epóxi preta que encapsula a matriz de silício (KÖMMERLING; KUHN, 1999).

Figura 3.8 – O ácido nítrico fumegante aquecido (> 98% HNO_3) dissolve a embalagem sem afetar o chip.

Fonte: Adaptado de Kömmerling.

As camadas são removidas camada por camada para expor as camadas subjacentes, sendo estes fotografadas para que essas imagens parciais sejam montadas e estudadas (SCHOBERT, 2010), baseado na especificação padrão de projeção e *layout* de CIs. Porém as especificações são valida porque se aplica à grande maioria dos CIs, o que facilita ao atacante um maior entendimento como se mostra na Figura 3.9[1].

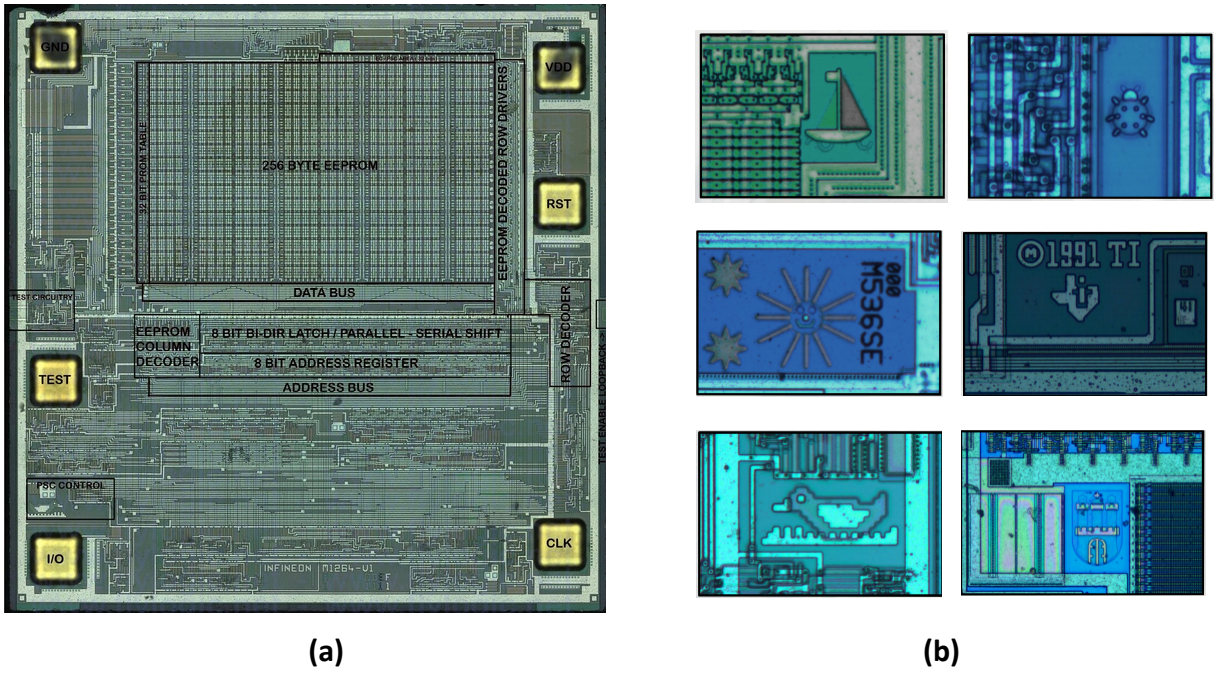


Figura 3.9 – Descapsulamento dos CIs (a) diagramas internas de um carão SIM e (b) logotipos de proteção de CIs.

Fonte: Adaptado de Martin Schobert e arquivo privado de M. janke, P. Laackmann.

Um invasor com acesso a equipamentos de teste de semicondutores pode recuperar informações importantes de um chip de cartão inteligente, investigando e manipulando diretamente os componentes do chip (ANDERSON; KUHN, 1996). Acreditamos que dado um investimento suficiente, qualquer dispositivo resistente a adulterações pode ser acessado e recuperado. Os pesquisadores de segurança de CI da Infineon M.Janke. e P.laackmann mostraram as técnicas de acesso ao CI, ilustrado na Figura 3.9b, onde se observa claramente os logotipos de proteção dos CIs, o que permitiria fazer a engenharia reversa.

Desta maneira, neste projeto de pesquisa criou-se uma estratégia para evitar este tipo de ataques. Para tanto, foi implementado na camada superior do layout do CI uma malha resistiva para dificultar o acesso e a analise dos atacantes. A malha resistiva com unidade de geração de chave é baseada na taxa de variação do nível de tensão na malha resistiva. Na Figura 3.10, mostra a malha resistiva (linha verde e azul) do sensor proposto,

[1] A diagrama interno de um cartão SIM Fonte: <https://www.quora.com/What-does-a-diagram-of-the-internals-of-a-SIM-card-look-like>

onde a linha vermelha (sensor) verifica durante a operação se existe interrupções ou curtos-circuitos, que por sua vez acionam os alarmes.

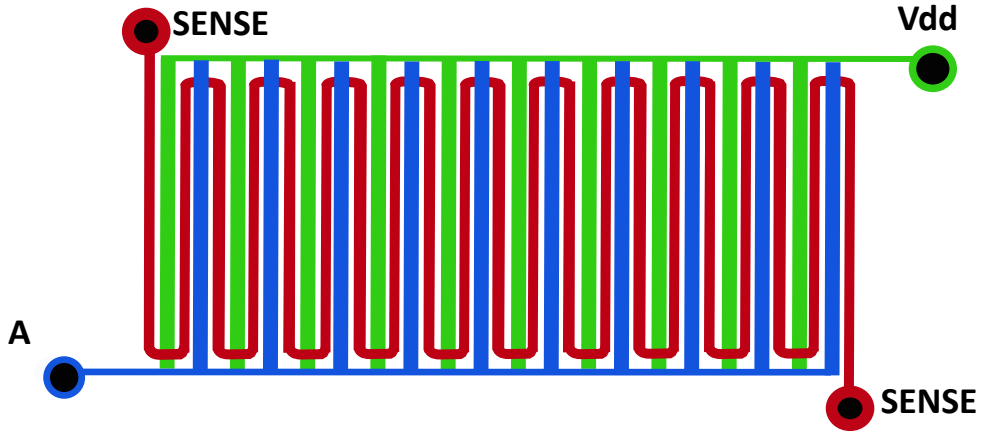


Figura 3.10 – Malha do sensor na última camada superior.

Fonte: Elaborado pelo autor.

4 ANÁLISES E RESULTADOS

Este capítulo apresenta as simulações das arquiteturas projetadas dos sensores protetores de CI de cartão inteligente (descrito no Capítulo 2) de ataques não invasivos e invasivos (mencionado no Capitulo 1) que são detalhados dentro dos tipos de ataques (Seção 2.1.5). Um dos ataques não invasivos mais comuns é a variação de temperatura nos extremos da faixa de operação. Para este tipo de ataques é projetado o sensor protetor de ataques de temperatura, o qual é composto dos seguintes circuitos: um gerador de tesão CTAT, dois comparadores e um controle lógico (como mencionado no diagrama de blocos da Figura 3.1). Cada um desdes circuitos é simulado e analisado separadamente para logo ser integrado, como um sensor protetor em temperatura. Além disso dentre os ataques invasivos, um dos mais comuns é de *Microprobing* ataque com acesso direto ao chip (detalhado na Seção 3.3). Para este tipo de ataques foi projetado uma malha resistiva como uma chave, baseada na taxa de variação do nível de tensão na malha resistiva, este sensor é composta de um circuito resistivo e um comparador.

As simulações destas arquiteturas foram feitas usando o Cadence Virtuoso da *Design Kit* 180 nm da tecnologia CMOS, e com modelo definido pela *Foundry* TSMC. Para que os resultados sejam mais estáveis e com menor margem de erro, cada arquitetura que conforma o circuitos sensor protetor foi simulado entre os $-40\,^{\circ}\mathrm{C}$ e $140\,^{\circ}\mathrm{C}$. Assim, desta forma pode garantir a eficiência da proposta inicial do sensor colocando-o como característica que o sensor está a prova de temperaturas extremas entre $-20\,^{\circ}\mathrm{C}$ e $120\,^{\circ}\mathrm{C}$, que são descritos a partir da Seção 4.1. Posteriormente é mostrado o posicionamento estratégico de *layout* do sensor protetor de ataques de temperatura e ataques invasivos (resistivo), no *layout* do CI de cartão inteligente.

Abaixo são apresentadas as especificações gerais que são utilizados nas simulações projetadas e as descrições de entradas e saídas dos blocos.

Especificações para a simulação dos circuitos projetados

Para realizar a análise das simulações utilizou-se o Cadence Virtuoso com DFM da *Design Kit* de processo TSMC 180 nm (pdk) da tecnologia CMOS. Cada componente destas arquiteturas foi simulada com os processos típicos de *corners* da seguinte maneira: para os componentes MOS com a configuração lento-rápido-lento-rápido sfsf (*slow-fast-slow-fast*), sffs, fssf, fsfs; e para os componentes resistivos, capacitores, BJT e Diodo com as configuração sf, fs, ss, ff. Considerando as configurações descritas para todos os circuitos que compõem os sensores protetores (gerados por falhas e de ataques *Microprobing* – acesso direto a superfície do chip).

Descrições de entradas e saídas (I/O) dos blocos

Para as simulações de teste são definidas os nomes das I/O com suas descrições, assim como para o esquemático e o *layout*; se lista brevemente na seguinte Tabela 4.1, para facilitar a integração com outros blocos que contém o CI de cartão inteligente.

Tabela 4.1 – Lista de entradas e saídas (I/O) dos blocos de arquitetura do Sensor Protetor (SP).

Nome	**Descrição**	**Tipo**	**Notas de Layout**
VDDA	Tensão de alimentação regulada	INOUT	
GNDA	Terra analógica de SP	INOUT	
OUT_TP	Output SP	OUT	
IN_500nA	Corrente de referência de entrada	INPUT	
cvref_400mV	Tensão de referência de entrada	INOUT	
cvref_700mV	Tensão de referência de entrada	INOUT	
OUT_CTAT	Saída de temperatura CTAT	OUT	Connected
IN_CTAT	Entrada de temperatura CTAT	INPUT	together

Fonte: Elaborado pelo autor.

4.1 Simulação de circuito gerador de tensão do sensor CTAT

Foi referido anteriormente no Capitulo 2 (Seção 2.2.1), que os transistores de junção bipolar apresentam menor sensibilidade aos fatores que tem os transistores CMOS, em base nisso são estudadas as arquiteturas para a geração tensão CTAT (Seção 2.2.2), PTAT (Seção 2.2.3) e circuitos que variam pouco com amplas faixas de temperatura (Seção 2.2.4). Baseado nessas arquiteturas foi proposta uma nova arquitetura (Seção 3.1) a fim de atingir as baixas e altas temperaturas.

Essa nova arquitetura sensor CTAT completa é mostrada na Figura 4.1, com todos os transistores necessários para o layout, sendo que foram feitas diversas simulações e ajustes aos tamanhos para se obter o melhor resultado possível. O sensor além das especificações descritas para a simulação requer de uma tensão DC 1,2 V e uma corrente de referência (iref_500nA) externa de 500 nA para gerar a tensão CTAT. Além de gerar uma tensão CTAT (V_Temp), gera duas correntes de referência $iref1\_1u$ =1 uA e $iref2\_1u$ =1 uA para os dois comparadores mostrados na Seção 4.2.

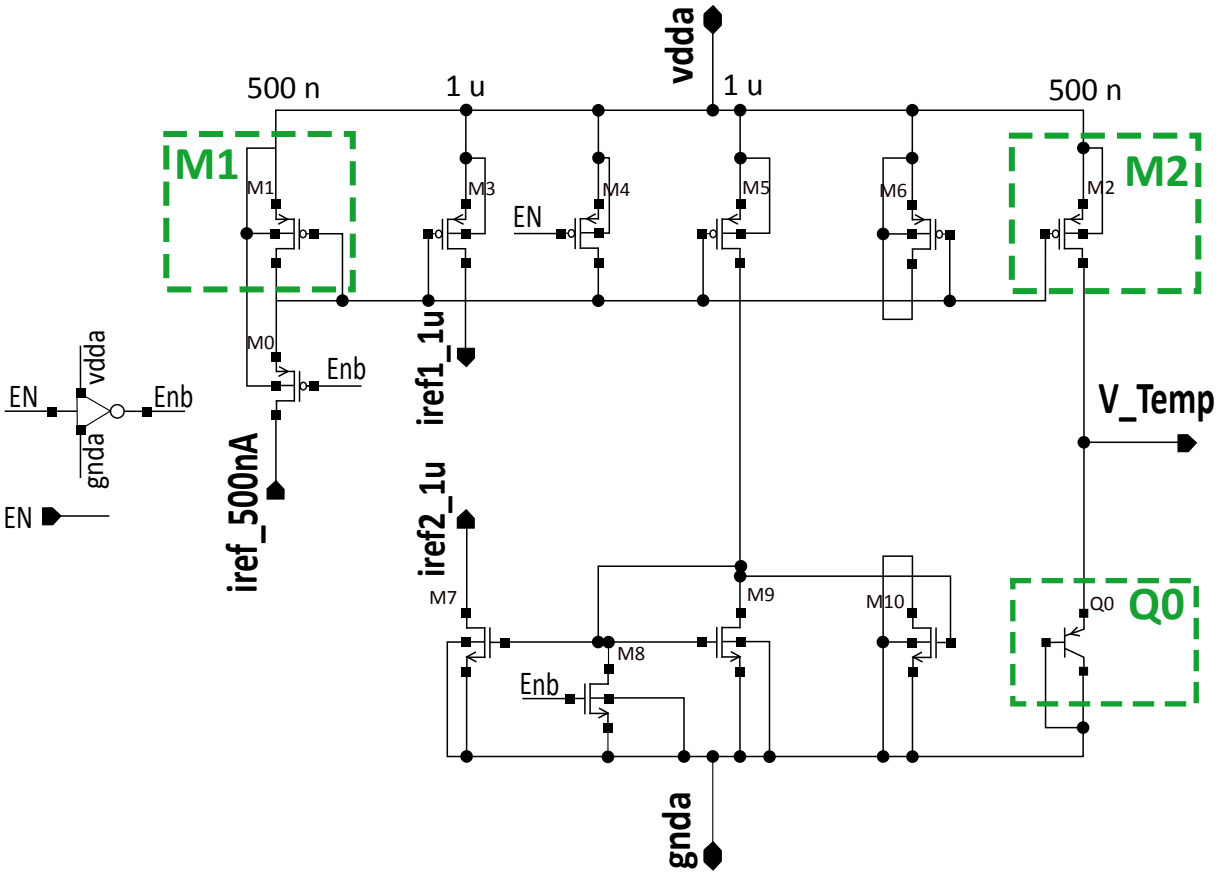


Figura 4.1 – Sensor de temperatura final para o layout.

Fonte: Projetado pelo autor.

A Figura 4.2 mostra os resultados da simulação da Figura 4.1 com as especificações mencionados nesta seção, efetuou-se a análise DC, STB (análise de estabilidade) de $-40\,°C$ a $140\,°C$ de temperatura e a variação $I_{ref} = 450\,nA$ a $550\,nA$, e V_{dd} =1,08 V a 1,32 V, e com o comando *.step temp* entre $-50\,°C$ e $150\,°C$, no Apêndice B.1 é apresentado o circuito de simulação.

Os resultados obtidos da simulação do sensor CTAT (Figura 4.2), mostram um excelente desempenho, com o que verificou-se o objetivo de calibração proposta na Seção 3.1 de obter a $-20\,°C$ uma voltagem de 700 mV e a $120\,°C$ uma voltagem de 400 mV, com uma pequena variação nesses limites como se mostra na Tabela 4.2, atingido satisfatoriamente a linealidade proposta nessas faixas de temperatura.

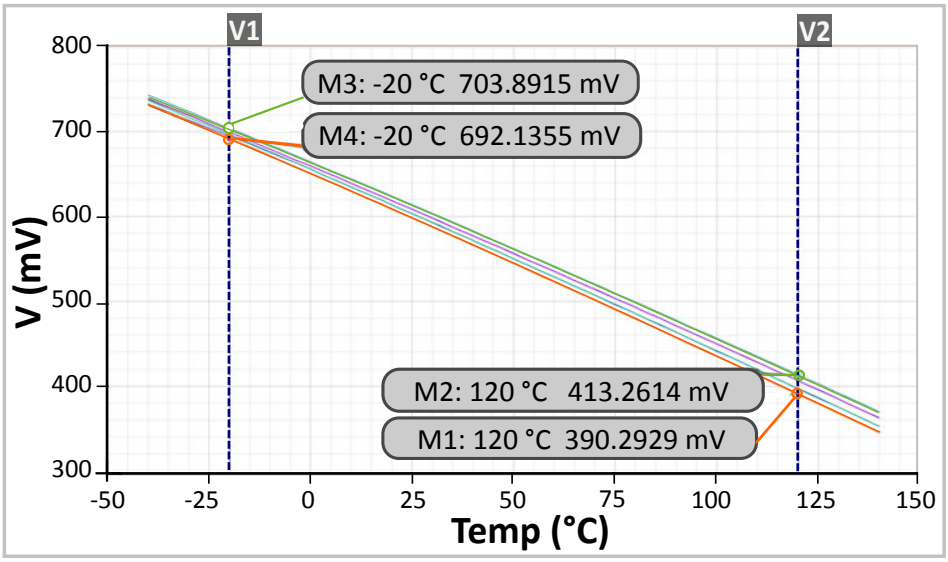


Figura 4.2 – Resultados de simulação de sensor CTAT no domínio da temperatura nas bordas (*Corner*).

Fonte: Projetado pelo autor.

Tabela 4.2 – Variação do sensor CTAT em *Corners*.

Temperatura	**Variação de voltagem**		
Celsius	V_{max} ***(mV)***	V_{min} ***(mV)***	ΔV ***(mV)***
−20 °C	703.98	692.13	11.85
120 °C	413.26	390.29	22.97

Fonte: Elaborado pelo autor.

4.1.1 Pontos de operação do sensor de temperatura em *corners*

Analisou-se também os pontos de operação do sensor CTAT (Figura 4.1), nos transistores principais M1 e M2 que conforma o sensor em sim, para comprovar a saturação dos mesmos nos piores casos, com as seguintes especificações: $Vdsat = Vgs - Vt > 100\,\text{mV}$ e $Von > 0\,\text{V}$, que deveriam atingir para o perfeito funcionamento destes transistores. Os pontos de operação em *corners* são mostrados na Tabela 4.3 onde podemos ver que M1 (Vsadt = 367,3 mV e Von=25,43 mV) e M2 (Vsadt = 367,3 mV e Von = 25,45 mV), atingem as especificações propostas.

Para garantir a estabilidade de este sensor CTAT, foi simulado, o PSRR (*Power supply Rejection Ratio*) razão de rejeição da fonte de alimentação, obtendo-se um valor de -62.043 dB no pior dos casos como se mostra na Figura 4.3, com o que é comprovado a estabilidade do sensor.

Tabela 4.3 – Análise nas bordas do sensor de temperatura dos 2 transistores.

	Output	Min	Max	Mean	Median	Stddev	Spec
M1	Vdsat_M1	367.3m	430.8m	399m	398.9m	25.34m	>100m
M1	Von_M1	25.43m	44.52m	334.8m	34.83m	6.727m	>0
M2	Vdsat_M2	387.1m	649.2m	517.4m	517.9m	119.6m	>100m
M2	Von_M2	25.45m	44.6m	34.85m	34.88m	6.722m	>0

Fonte: Elaborado pelo autor.

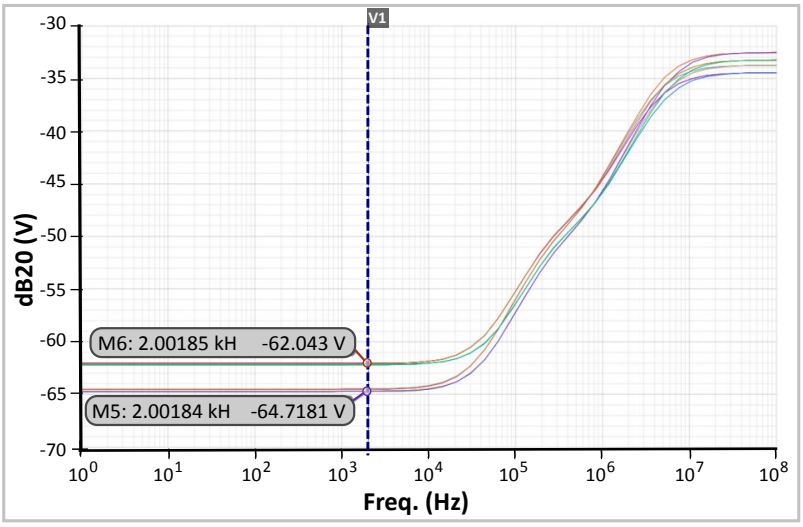


Figura 4.3 – Análise de PSRR no sensor de temperatura do *corner*.

Fonte: Projetado pelo autor.

4.2 Simulação dos comparadores de tensão diferencial com arquitetura de histerese

Os comparadores projetados para os sensores protetores (sensor protetor de ataques com variação de temperatura e sensor resistivo a adulteração para CI de cartão inteligente), são os comparadores com histereses devido a vantagem que tem comparado com aqueles sem histereses (Seção 3.2.1). Esses comparadores são projetados também com um mínimo número de transistores como se mostra na Figura 4.4, para ser integrados com o sensor CTAT, para ter um controle nos valores especificados de proteção nos limites superior e inferior de temperaturas. Onde os transistores M7/M8 da Figura 4.4b é um par diferencial PMOS com $V_{in}+ = V_{ref1} = 400\,\text{mV}$ para a proteção acima da temperatura de 120 °C, da mesma forma os transistores M15/M16 da Figura 4.4a é um par diferencial NMOS com $V_{in}+ = V_{ref2} = 700\,\text{mV}$ para a proteção abaixo da temperatura de $-20\,°\text{C}$.

Para o caso de comparadores assim como foi analisado nos sensores CTAT, também precisou-se fazer uma análise em DC com uma tensão $V_{dd} = 1{,}2\,\text{V} \pm 10\%$ e uma corrente de referência externa de 1 uA, fornecida por o sensor CTAT (com todas as especificações e ajustes feitos no sensor CTAT) para polarizar os transistores dos comparadores de par diferencial PMOS e NMOS, no Apêndice C.1 é apresentado o circuito de simulação destes comparadores.

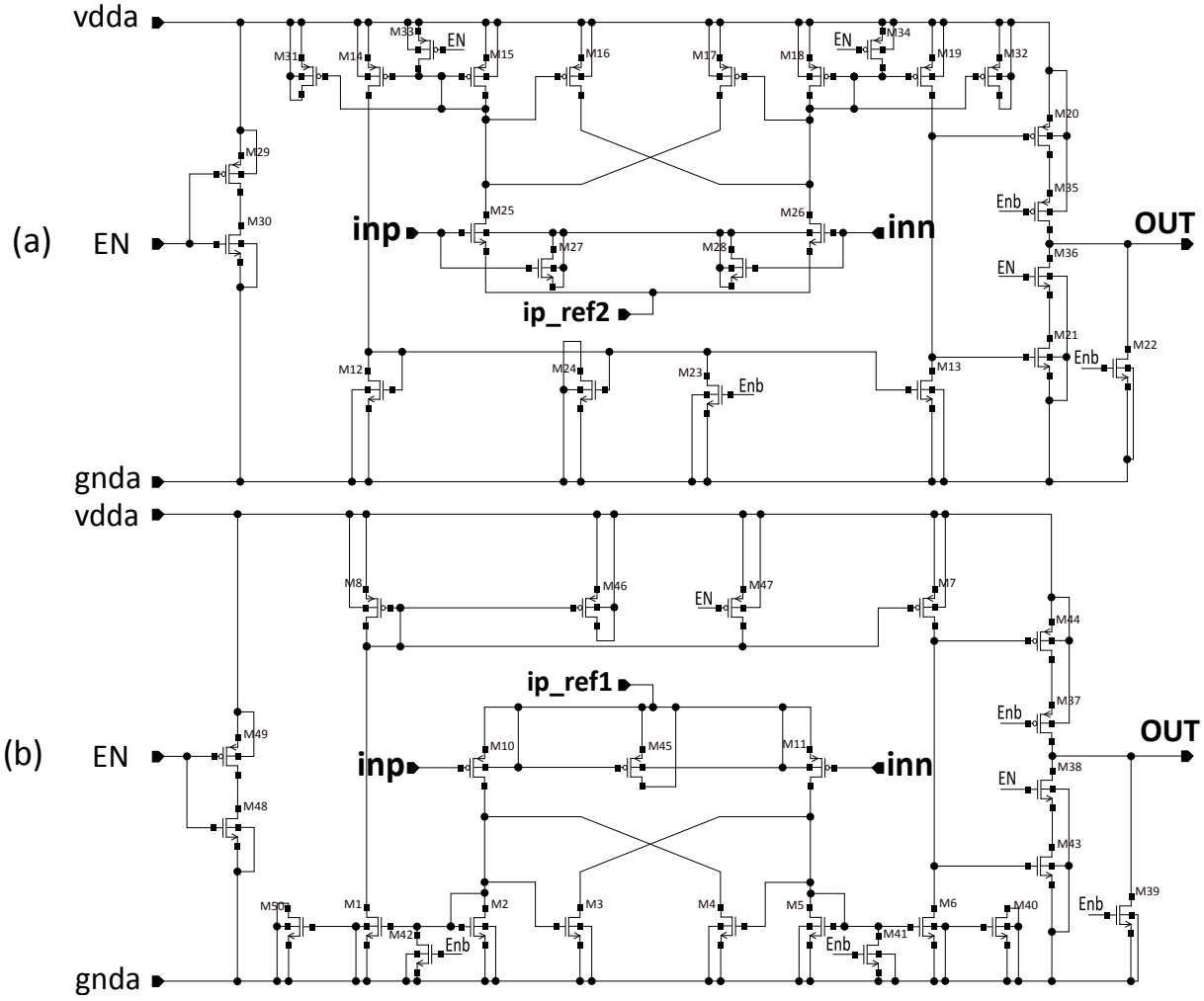


Figura 4.4 – Esquemático dos comparadores com histereses: (a) comparador de par diferencial NMOS e (b) comparador de par diferencial PMOS.

Fonte: Projetado pelo autor.

Os melhores resultados das simulações em *corners* conseguidos com estas arquiteturas é apresentada na Figura 4.5. Analisando este resultado podemos observar que as variações de histereses são de 7 mV para os limites de temperatura com as faixas de tenção 700 mV e 400 mV o que significa que está dentro das especificações da proposta para ter uma melhor controle de comparação.

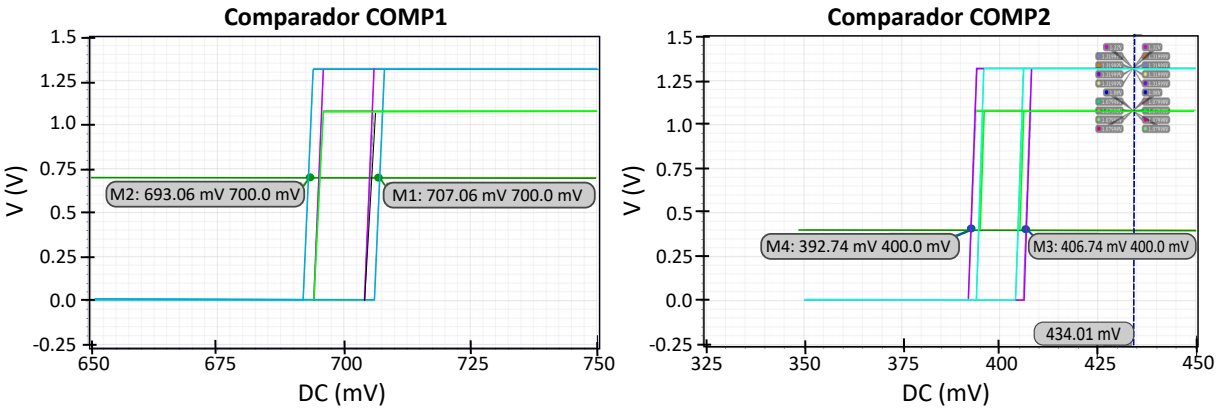


Figura 4.5 – Resultados da simulação dos comparadores: comparador par diferencial NMOS (a) e comparador par diferencial PMOS (b).

Fonte: Projetado pelo autor.

4.3 Simulação de circuito protetor de ataques de adulteração

Estudos demonstram que não existe segurança absoluta contra ataques invasivos. Mas fazendo uso de recursos modernos de proteção de CI que incluem sensores internos, podem proteger contra ataques de criptografia de hardware de barramento interno para tornar a análise de dados mais difícil. Para tal foi projetado um sensor resistivo que consiste em uma malha resistiva posicionada na camada superior do CI. Todos os caminhos dessa malha foram monitorados continuamente para ter maior controle dos ataques.

Com o intuito de criar um sensor resistivo conectado no mesmo sensor de temperatura, foi projetado um circuito sensor resistivo (ver Figura 4.6) que possui como entrada apenas uma alimentação de 1,2 V e a polarização retirado do sensor CTAT V_{G-M1} para controlar a passagem da corrente no transistor M3 e a resistência $R = 50\,\mathrm{K\Omega}$ é malha resistiva. Assim, desta forma, pode-se obter uma proteção em temperatura e resistivo.

Este circuito é simulado com as especificações dada nesta seção e com as mesmas configurações do que o sensor CTAT entre $-40\,^{\circ}\mathrm{C}$ e $140\,^{\circ}\mathrm{C}$, com fonte de tensão DC de $1{,}2\,\mathrm{V} \pm 10\%$ e corrente de referência variando de 450 nA a 550 nA.

Os resultados da simulação de resistência à adulteração em DC, resistência vs tensão é mostrada na Figura 4.7, ao quebrar os resistores em paralelo a resistência aumenta variando a tensão na saída, isso é comparado com a tensão de referência *bandgap* de 700 mV, que consequentemente direciona o circuito para a redefinição ou zeramento da memória EEPROM do chip.

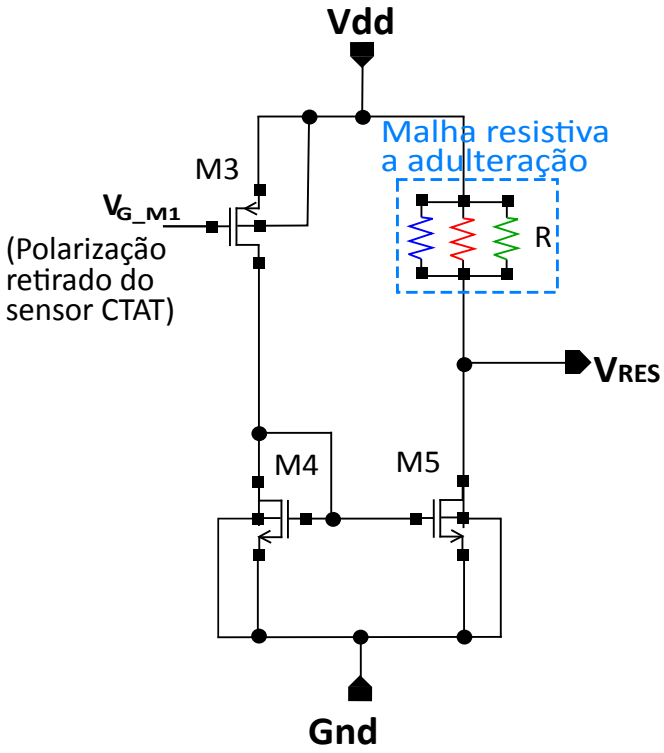


Figura 4.6 – Sensor resistivo a adulteração.

Fonte: Projetado pelo autor.

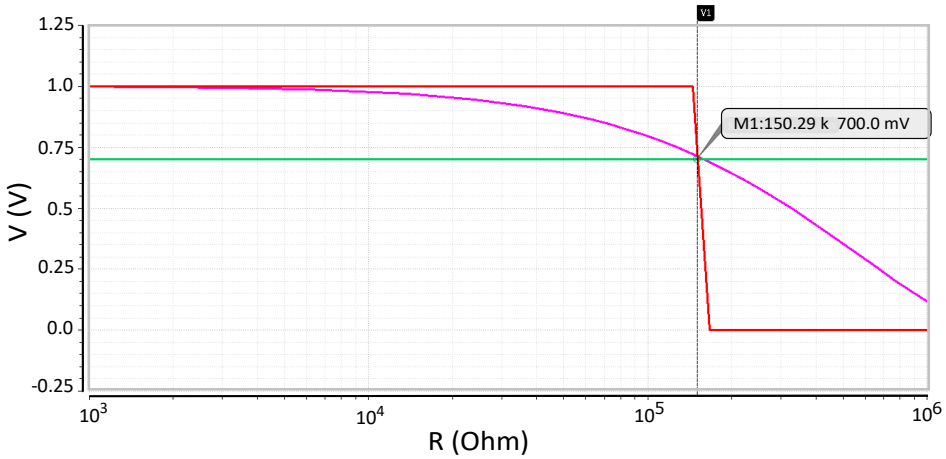


Figura 4.7 – Simulação de *corners* do sensor resistivo proteção a adulteração.

Fonte: Projetado pelo autor.

4.4 Simulação da arquitetura do sensor protetor de ataques em temperatura do CI de cartões inteligentes

Para a simulação e integração do sensor completo com outros blocos de CI de cartão inteligente, foi criado um símbolo que é mostrado na Figura 4.8, onde é possível observar todos os blocos projetados e descritos anteriormente neste relatório como mostrada a Figura 4.9, contendo o bloco sensor CTAT juntamente com as bias do mesmo, os dois comparadores e finalmente o circuito de controle logico, responsável pela decisão de ativar e desativar o sensor protetor de CI de cartão inteligente.

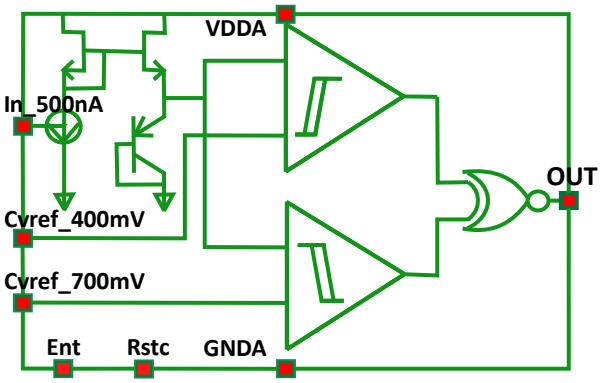


Figura 4.8 – O simbolo de sensor protetor em temperatura.

Fonte: Elaborado pelo autor.

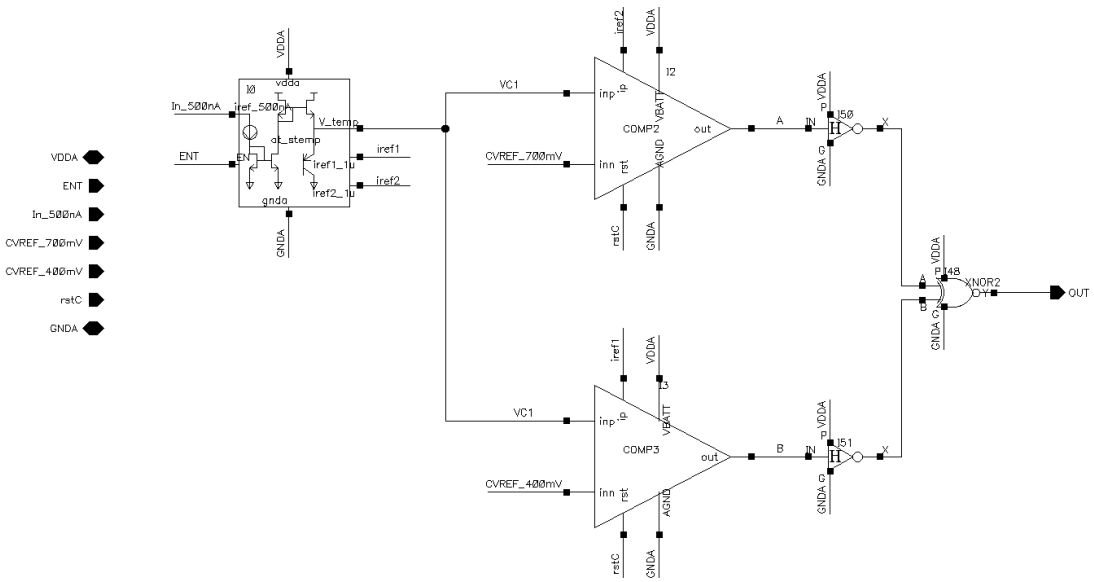


Figura 4.9 – Esquemático global do sensor protetor de temperatura.

Fonte: Projetado pelo autor.

Para o correto funcionamento do circuito além da alimentação são necessários: Sinal de *Reset* (Rstc), uma corrente de referência I_{ref} =500 nA e tensões de referência V_{ref1} =400 mV e V_{ref2} =700 mV para o controle de variação de tensão nos limites de temperatura de −20 °C a 120 °C. Atribuíção destes valores para a simulação estão especificadas no Apêndice D.1.

Na Figura 4.10 é apresentada uma simulação em *corners* para a totalidade do sensor de temperatura protetor de CIs de cartões inteligentes, onde são apresentados diversos sinais, sendo o mais importante o resultado obtido da simulação nas condições de temperatura extrema de −40 °C a 140 °C, V_{dd} = 1,2 V±10% e I_{ref} = 450 nA a 550 nA mostra um intervalo muito linear.

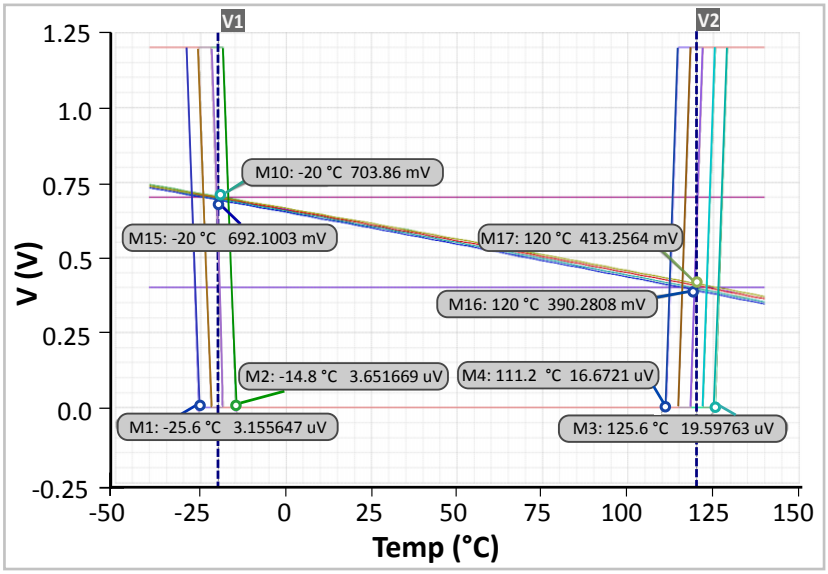


Figura 4.10 – Simulações do *corner* da proteção de sensor de temperatura.

Fonte: Projetado pelo autor.

Através da Figura 4.10 é possível analisar o comportamento do sistema. O sinal em tensão do sensor tem uma variação pequena como se mostra na Tabela 4.4, mas em análises em temperatura o que o objetivo central desta pesquisa, observa-se que nas faixas menores a −25 °C (700 mV) e maiores a 125 °C (400 mV) a saída (OUT) vai para alto (1,2 V), anunciando a ameaça, bloqueando a operação do CI de cartão inteligente, mas sim está na faixa entre −25 °C (700mV) a 115 °C (400mV) o sinal esta em baixo (0V) o que avisa ao CI que esta sem ameaça e o CI faz as operações com toda segurança. Portanto, o circuito mostra um excelente desempenho geral, especialmente em relação à linearidade para o intervalo de temperatura −20 °C a 120 °C.

Tabela 4.4 – Variações de tensão de sensor proteção de temperatura em *Corners*.

Temperatura	**Variação de voltagem**		
Celsius	V_{max} **(mV)**	V_{min} **(mV)**	ΔV **(mV)**
−20 °C	703.86	692.10	11.76
120 °C	413.25	390.28	22.97

Fonte: Elaborado pelo autor.

4.5 Posição de layout do sensor de temperatura para proteção de CIs

O sensor de temperatura que se propõe nesta pesquisa pode ser usado em diferentes posições no *layout* do chip do CI de cartões inteligentes. Então, esse posicionamento deve ser em áreas estratégicas sujeita a aquecimento (baseado em casamento de transistores), para melhorar a proteção dos transistores. Consequentemente obtemos o sensor alocado no nível superior do *layout* como se ilustra na Figura 4.11 do CI.

No caso do sensor resistivo (malha) o posicionamento é na camada superior do *layout* para dificultar o decapsulação do CI, funcionando como chave sensível à intrusão.

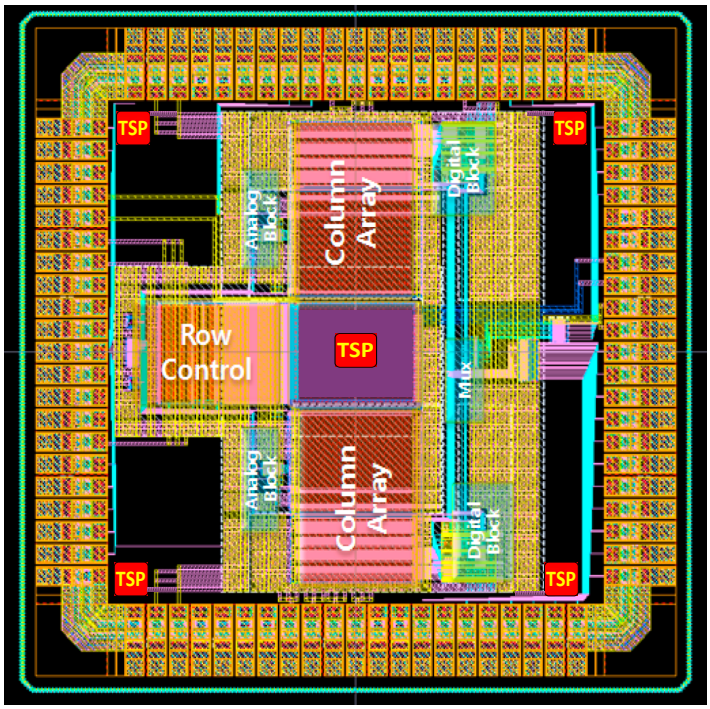


Figura 4.11 – Posição do circuito do sensor de temperatura nos circuitos integrados.

Fonte: Elaborado pelo autor.

4.6 Comparação com outros trabalhos

Conforme demostrado pelos resultados da simulação das arquiteturas do sensor projetado, o circuito sensor CTAT, é um sensor de temperatura que poderia ser comparado com o estado da arte, como é mostrado na Tabela 4.5. Uma comparação justa principalmente em relação a tecnologia, potência de consumo, erro porcentual e a faixa de operação dos sensores simulados desde o ano 2013 até a atualidade.

Tabela 4.5 – Comparação com outros trabalhos

Trabalhos	**Tecnologia**	**Potência (µW)**	**Erro (°C)**	**Faixa de T.**
Souri K. (ISSCC) 2013 (SOURI; CHAE; MAKINWA, 2013)	0.16µm	6.8	± 0.15	[−55 °C, 125 °C]
Chen Zhao (ISCAS) 2013 (ZHAO et al., 2013)	0.18µm	1.026	0.21	[−20 °C, 100 °C]
Fabio Sebastiano (JSSC) 2010 (SEBASTIANO et al., 2010)	65nm	9.96	0.2	[−75 °C, 125 °C]
Jung Oh-Yong (ISCAS) 2013 (JUNG et al., 2013)	0.13µm	2	0.048	[20 °C, 50 °C]
C Azcona (ISCAS) 2015 (AZCONA et al., 2015)	0.18µm	1.35	± 0.66	[−40 °C, 120 °C]
Xiao Pu (JSSC) 2015 (PU et al., 2015)	65nm	0.9	± 0.4	[−40 °C, 130 °C]
Yuze Niu1. (ASICON) 2017 (NIU et al., 2017)	0.18µm	1.35	± 0.1	[−40 °C, 85 °C]
Luis Cartagena. (IMOC) 2017 (CARTAGENA; BARBIN, 2017)	90nm	0.6	0.0325	[−20 °C, 120 °C]
L. Cartagena. (LAMC) 2018 (CARTAGENA; BARBIN; SALCEDO, 2018)	180nm	0.6	0.0325	[−20 °C, 120 °C]
Kim H. (Sensors and Materials) 2019 (KIM et al., 2019)	180nm	19.72	–	[−10 °C, 80 °C]

Fonte: Elaborado pelo autor.

Em comparação com outras arquiteturas, nossa topologia tem potência de consumo e margem de erro menor com outros trabalhos publicados. O desempenho do circuito sensor tem uma linearidade boa nessa faixa de operação. Desta maneira, se mostra que o sensor poderia ser integrado facilmente com outros circuitos. A miniaturização dos sensores de temperatura baseados em BJT também é uma importante contribuição em nosso trabalho. Os meios de reduzir a área da matriz e simultaneamente reduzir o consumo de energia do sensor de temperatura foi um dos desafios desta pesquisa.

5 CONCLUSÕES E TRABALHOS FUTUROS

O crescente uso de cartões inteligentes nas variadas atividades das pessoas individuais, sistemas coletivos e companhias tem tornado este tipo de dispositivos de uso cotidiano, por este motivo os CIs de cartões inteligentes são alvos de ataques sendo o mais agressivo, o ataque dos canais laterais ativados quando a temperatura de operação dos CIs esta o limite extremo de seu ponto de operação, Nesse sentido no presente trabalho foi proposto um sistema de proteção de cartões inteligentes baseado num sensor de temperatura de baixa potência na faixa de $-20\,°C$ a $120\,°C$. Para tal fim foi projetado um sistema sensor de temperatura de área pequena e de baixo consumo de energia. O sensor foi projetado em Cadence usando o conceito *System-on-a-Chip* (SoC) na tecnologia padrão CMOS de 0,18 µm que opera com uma tensão de alimentação de 1,2 V. O Sensor de temperatura é baseado em um circuito com dois transistores CMOS (*Complementary Metal Oxide Semicondutor*) e um transistor bipolar PNP para produzir uma tensão CTAT (*Complementary To Absolute Temperature voltage*). O resultado obtido da simulação nas condições de temperaturas extremas de $-40\,°C$ a $140\,°C$ e $V_{dd} = 1{,}2\,V \pm 10\%$, mostram um excelente desempenho para o sensor; com uma taxa de rejeição da fonte de alimentação PSRR (*Power supply rejection ratio*) $-62\,dB$ no pior dos casos e com histerese de 5 mV. Este novo design de circuito pode efetivamente funcionar como um excelente protetor contra adulteração de segurança em cartões inteligentes.

Trabalhos futuros

Os resultados apresentados até aqui abrem caminhos de possibilidades para avanço da pesquisa, tanto através da continuidade como a integração dos dois sensores em um só, e também para a implementação de proteção dos outros tipos de ataques mencionados nesta pesquisa, devido que a proteção é uma batalha contínua dentre fabricantes que inventam novas soluções de segurança, aprendendo suas lições com erros anteriores e a comunidade de *hackers* constantemente tentando quebrar as proteções implementadas.

5.1 Contribuições e publicações

Durante o período da pesquisa participou-se na publicação de artigos científico:

Artigo publicado

- "A New Sensor for Temperature Self-Protection of Integrated Circuits in CMOS Technology"
  CARTAGENA, Luis Q.; BARBIN, Silvio E.; SALCEDO, Walter J. A New Sensor for Temperature Self-Protection of Integrated Circuits in CMOS Technology. In: **2018 IEEE MTT-S Latin America Microwave Conference (LAMC 2018).** IEEE, 2018. p. 1-4.
  <https://ieeexplore.ieee.org/document/8699058/>

- "Low Power CMOS Thermal and Tamper Sensor for Smart Cards Protection"
  CARTAGENA, Luis; BARBIN, Silvio. Low Power CMOS Thermal and Tamper Sensor for Smart Cards Protection. In: **International Conference on Electromagnetics in Advanced Applications (ICEAA), 2018**. IEEE Conference, 2018. p. 671-674.
  <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8520486>

- "Low power CMOS temperature protection sensor for smart cards"
  CARTAGENA, Luis; BARBIN, Silvio. Low power CMOS temperature protection sensor for smart cards. In: **Microwave and Optoelectronics Conference (IMOC), 2017 SBMO/IEEE MTT-S International**. IEEE, 2017. p. 1-5.
  <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8121153>

Além disso, há artigo em fase de publicação e redação que deve ser apresentados posteriormente.

Artigo em fase de desenvolvimento

- "Magnetic and Power protection for Smart Cards in CMOS"

REFERÊNCIAS

ALLEN, P. E.; HOLBERG, D. R. **CMOS analog circuit design**. [S.l.]: Oxford university press, 2012. Citado na página 44.

ALLSTOT, D. J. A precision variable-supply cmos comparator. **IEEE Journal of Solid-State Circuits**, IEEE, v. 17, n. 6, p. 1080–1087, 1982. Citado na página 44.

ANDERSON, R.; KUHN, M. Tamper resistance-a cautionary note. In: **Proceedings of the second Usenix workshop on electronic commerce**. [S.l.: s.n.], 1996. v. 2, p. 1–11. Citado nas páginas 17, 24, 30, 31 e 47.

ANDERSON, R.; KUHN, M. Low cost attacks on tamper resistant devices. In: SPRINGER. **International Workshop on Security Protocols**. [S.l.], 1997. p. 125–136. Citado na página 17.

ANJALI, K.; RAO, R. V. An energy efficiency systematic cell design methodology using inputs xor & xnor. **IJMTST International Journal for Modern Trends in Science and Technology**, IJMTST, v. 02, p. 102–105, 2016. Citado na página 45.

AZCONA, C. et al. A 1.2-v 1.35-v;w all mos temperature sensor for wireless sensor networks. In: **IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS)**. [S.l.: s.n.], 2015. p. 365–368. ISSN 0271-4302. Citado na página 60.

BAKKER, A.; HUIJSING, J. H. Micropower cmos temperature sensor with digital output. **IEEE Journal of Solid-State Circuits**, IEEE, v. 31, n. 7, p. 933–937, 1996. Citado na página 17.

BAR-EL, H. et al. The sorcerer's apprentice guide to fault attacks. **Proceedings of the IEEE**, IEEE, v. 94, n. 2, p. 370–382, 2006. Citado na página 15.

BIN, Z.; QUAN-YUAN, F. A novel thermal-shutdown protection circuit. In: IEEE. **3rd INTERNATIONAL CONFERENCE ON ANTI-COUNTERFEITING, SECURITY, AND IDENTIFICATION IN COMMUNICATION**. [S.l.], 2009. p. 535–538. Citado na página 40.

CARTAGENA, L.; BARBIN, S. Low power cmos temperature protection sensor for smart cards. In: IEEE. **Microwave and Optoelectronics Conference (IMOC), 2017 SBMO/IEEE MTT-S International**. [S.l.], 2017. p. 1–5. Citado na página 60.

CARTAGENA, L. Q.; BARBIN, S. E.; SALCEDO, W. J. A new sensor for temperature self-protection of integrated circuits in cmos technology. In: IEEE. **IEEE MTT-S LATIN AMERICA MICROWAVE CONFERENCE (LAMC 2018)**. [S.l.], 2018. p. 1–4. Citado na página 60.

CHENG, Y.; HU, C. **MOSFET modeling & BSIM3 user's guide**. [S.l.]: Springer Science & Business Media, 1999. Citado na página 32.

DAVIDSON, A.; BUIS, A.; GLESK, I. Toward novel wearable pyroelectric temperature sensor for medical applications. **IEEE Sensors Journal**, IEEE, v. 17, n. 20, p. 6682–6689, 2017. Citado na página 18.

DENG, C. et al. A cmos smart temperature sensor with single-point calibration method for clinical use. **IEEE Transactions on Circuits and Systems II: Express Briefs**, IEEE, v. 63, n. 2, p. 136–140, 2015. Citado na página 40.

DESCENT, P.; IZQUIERDO, R.; FAYOMI, C. Printing of temperature and humidity sensors on flexible substrates for biomedical applications. In: IEEE. **IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS)**. [S.l.], 2018. p. 1–4. Citado na página 18.

DULAU, L. et al. A new gate driver integrated circuit for igbt devices with advanced protections. **IEEE Transactions on Power Electronics**, IEEE, v. 21, n. 1, p. 38–44, 2006. Citado na página 17.

GARULLI, N. et al. A low power temperature sensor for iot applications in cmos 65nm technology. In: IEEE. **IEEE 7TH INTERNATIONAL CONFERENCE ON CONSUMER ELECTRONICS-BERLIN (ICCE-BERLIN**. [S.l.], 2017. p. 92–96. Citado na página 18.

HENDRY, M. **Multi-application smart cards: technology and applications**. [S.l.]: Cambridge university press, 2007. Citado na página 20.

HILLEBRAND, F. **GSM and UMTS: the creation of global mobile communication**. [S.l.]: John Wiley & Sons, Inc., 2002. Citado na página 26.

HUTTER, M.; SCHMIDT, J.-M. The temperature side channel and heating fault attacks. In: SPRINGER. **INTERNATIONAL CONFERENCE ON SMART CARD RESEARCH AND ADVANCED APPLICATIONS**. [S.l.], 2013. p. 219–235. Citado na página 17.

JUNG, O. Y. et al. A low power low inaccuracy linearity-compensated temperature sensor for attachable medical devices. In: **IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS2013)**. [S.l.: s.n.], 2013. p. 1087–1090. ISSN 0271-4302. Citado na página 60.

KIM, H. et al. Stbc: Side channel attack tolerant balanced circuit with reduced propagation delay. In: **IEEE COMPUTER SOCIETY ANNUAL SYMPOSIUM ON VLSI (ISVLSI)**. [S.l.: s.n.], 2017. p. 74–79. Citado na página 16.

KIM, H. et al. Secure circuit with low-power on-chip temperature sensor for detection of temperature fault injection attacks. **Sensors and Materials**, v. 31, n. 5, p. 1375–1386, 2019. Citado na página 60.

KLAAS, J. **System-on-a-chip**. [S.l.]: Google Patents, 2004. US Patent 6,816,750. Citado na página 16.

KOCHER, P.; JAFFE, J.; JUN, B. Differential power analysis. In: SPRINGER. **ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE**. [S.l.], 1999. p. 388–397. Citado na página 31.

KÖMMERLING, O.; KUHN, M. G. Design principles for tamper-resistant smartcard processors. **Smartcard**, v. 99, p. 9–20, 1999. Citado nas páginas 17, 30 e 46.

LAUR, J.-P. et al. A new circuit-breaker integrated device for protection applications. In: IEEE. **11TH INTERNATIONAL SYMPOSIUM ON POWER SEMICONDUCTOR DEVICES AND ICS. ISPSD'99 PROCEEDINGS (CAT. NO. 99CH36312)**. [S.l.], 1999. p. 315–318. Citado na página 17.

LAW, M. K.; BERMAK, A.; LUONG, H. C. A sub-\ *muw* embedded cmos temperature sensor for rfid food monitoring application. **IEEE journal of solid-state circuits**, IEEE, v. 45, n. 6, p. 1246–1255, 2010. Citado na página 18.

MAES, H.; SIX, P.; SANSEN, W. The implanted zener diode (izd) as an input protection device for mos integrated circuits. **IEEE Transactions on Electron Devices**, IEEE, v. 28, n. 9, p. 1071–1077, 1981. Citado na página 17.

MAYES, K.; MARKANTONAKIS, K. **Smart Cards, Tokens, Security and Applications**. [S.l.]: Springer, 2017. Citado nas páginas 16 e 25.

NEUTEBOOM, H.; KUP, B. M.; JANSSENS, M. A dsp-based hearing instrument ic. **IEEE Journal of Solid-State Circuits**, IEEE, v. 32, n. 11, p. 1790–1806, 1997. Citado na página 38.

NIU, Y. et al. A low-power self-calibration digital-output cmos temperature sensor with x00b1;0.1 x00b0;c inaccuracy from x2212;40 x00b0;c to 85 x00b0;c. In: **IEEE 12TH INTERNATIONAL CONFERENCE ON ASIC (ASICON)**. [S.l.: s.n.], 2017. p. 1005–1008. Citado na página 60.

PERTIJS, M. A.; MEIJER, G. C.; HUIJSING, J. H. Precision temperature measurement using cmos substrate pnp transistors. **IEEE Sensors Journal**, IEEE, v. 4, n. 3, p. 294–300, 2004. Citado nas páginas 33, 39 e 42.

PU, X. et al. An embedded 65 nm cmos remote temperature sensor with digital beta correction and series resistance cancellation achieving an inaccuracy of 0.4^{circ}c ($3sigma$) from $-$ 40^{circ} c to 130^{circ} c. **IEEE Journal of Solid-State Circuits**, v. 50, n. 9, p. 2127–2137, Sept 2015. ISSN 0018-9200. Citado na página 60.

QUADIR, S. E. et al. A survey on chip to system reverse engineering. **ACM journal on emerging technologies in computing systems (JETC)**, ACM, v. 13, n. 1, p. 6, 2016. Citado na página 17.

RANKL, W. **Smart Card Applications: Design models for using and programming smart cards**. [S.l.]: John Wiley & Sons, 2007. Citado na página 22.

RANKL, W.; EFFING, W. **Smart card handbook**. [S.l.]: John Wiley & Sons, 2004. Citado nas páginas 20 e 22.

RAO, Y.-J. et al. In-fiber bragg-grating temperature sensor system for medical applications. **Journal of Lightwave Technology**, IEEE, v. 15, n. 5, p. 779–785, 1997. Citado na página 18.

RAZAVI, B. The bandgap reference [a circuit for all seasons]. **IEEE Solid-State Circuits Magazine**, IEEE, v. 8, n. 3, p. 9–12, 2016. Citado nas páginas 36 e 38.

REPORT, M. R. **Smart Card Materials Market Analysis Report By Material (PVC, Polycarbonate), By Type (Contact, Contactless, Multi-Component), By Application (Telecom, BFSI, Retail, Government), And Segment Forecasts, 2018 - 2025**. Augost 2018. <https://www.grandviewresearch.com/industry-analysis/smart-card-materials-market>. Access 30 November 2018. Citado na página 16.

SAXENA, A.; SHRIVASTAVA, A.; AKASHE, S. Low power, high speed schmitt trigger using svl technique in nanoscale cmos technology. **International Journal of Signal and Imaging Systems Engineering**, Inderscience Publishers (IEL), v. 9, n. 2, p. 85–94, 2016. Citado na página 44.

SCHAEFFER, P. L. et al. **A simple sub-1V voltage reference**. Tese (Doutorado), 2017. Citado nas páginas 38 e 39.

SCHOBERT, M. **STUDIENARBEIT: REVERSE-ENGINEERING VON LOGIK-GATTERN IN INTEGRIERTEN SCHALTKREISEN**. Dissertação (Mestrado) — Humboldt-Universität zu Berlin, 2010. Citado na página 47.

SEBASTIANO, F. et al. A 1.2-v 10-mu w npn-based temperature sensor in 65-nm cmos with an inaccuracy of 0.2 ^{circ} c (3$sigma$) from $-$ 70 ^{circ} c to 125 ^{circ} c. **IEEE Journal of Solid-State Circuits**, v. 45, n. 12, p. 2591–2601, Dec 2010. ISSN 0018-9200. Citado na página 60.

SHI, Q. et al. A layout-driven framework to assess vulnerability of ics to microprobing attacks. In: IEEE. **Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on**. [S.l.], 2016. p. 155–160. Citado nas páginas 15 e 17.

SKOROBOGATOV, S. How microprobing can attack encrypted memory. In: IEEE. **EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN (DSD)**. [S.l.], 2017. p. 244–251. Citado na página 17.

SKOROBOGATOV, S. P. **Semi-invasive attacks: a new approach to hardware security analysis**. Tese (Doutorado) — Citeseer, 2005. Citado nas páginas 17 e 30.

SMITH, M. On the circuit analysis of the schmitt trigger. **IEEE Journal of Solid-State Circuits**, IEEE, v. 23, n. 1, p. 292–294, 1988. Citado na página 44.

SOURI, K.; CHAE, Y.; MAKINWA, K. A. A. A cmos temperature sensor with a voltage-calibrated inaccuracy of pm 0.15^{circ} c (3$sigma$) from $-$ 55^{circ} c to 125^{circ} c. **IEEE Journal of Solid-State Circuits**, v. 48, n. 1, p. 292–301, Jan 2013. ISSN 0018-9200. Citado na página 60.

STÜBER, G. L. **Principles of mobile communication**. [S.l.]: Springer, 2017. v. 3. Citado na página 26.

TARNOVSKY, C. **From the eye of a legal storm, Murdoch's Satellite-TV Hacker tells all**. 2008. <https://www.wired.com/2008/05/tarnovsky/>. Access 22 November 2018. Citado na página 30.

TEHRANIPOOR, M.; WANG, C. **Introduction to hardware security and trust**. [S.l.]: Springer Science & Business Media, 2011. Citado nas páginas 16 e 17.

UENO, K. et al. Ultralow-power smart temperature sensor with subthreshold cmos circuits. In: IEEE. **INTERNATIONAL SYMPOSIUM ON INTELLIGENT SIGNAL PROCESSING AND COMMUNICATIONS**. [S.l.], 2006. p. 546–549. Citado na página 40.

WANG, H. et al. Probing attacks on integrated circuits: Challenges and research opportunities. **IEEE Design & Test**, IEEE, v. 34, n. 5, p. 63–71, 2017. Citado na página 17.

WANG, J.-M.; FANG, S.-C.; FENG, W.-S. New efficient designs for xor and xnor functions on the transistor level. **IEEE Journal of solid-state Circuits**, IEEE, v. 29, n. 7, p. 780–786, 1994. Citado na página 45.

WANG, X. et al. Role of power grid in side channel attack and power-grid-aware secure design. In: **50TH ACM/EDAC/IEEE DESIGN AUTOMATION CONFERENCE (DAC)**. [S.l.: s.n.], 2013. p. 1–9. ISSN 0738-100X. Citado na página 16.

WIDLAR, R. New developments in ic voltage regulators. In: IEEE. **SOLID-STATE CIRCUITS CONFERENCE. DIGEST OF TECHNICAL PAPERS. 1970 IEEE INTERNATIONAL**. [S.l.], 1970. v. 13, p. 158–159. Citado na página 36.

WIDLAR, R. J. New developments in ic voltage regulators. **IEEE Journal of Solid-State Circuits**, IEEE, v. 6, n. 1, p. 2–7, 1971. Citado na página 38.

WITTEMAN, M. Advances in smartcard security. **Information Security Bulletin**, v. 7, n. 2002, p. 11–22, 2002. Citado na página 15.

WOUDENBERG, J. G. V.; WITTEMAN, M. F.; MENARINI, F. Practical optical fault injection on secure microcontrollers. In: IEEE. **2011 Workshop on Fault Diagnosis and Tolerance in Cryptography**. [S.l.], 2011. p. 91–99. Citado na página 17.

YANG, Q. et al. Intense electric-field optical sensor for broad temperature-range applications based on a piecewise transfer function. **IEEE Transactions on Industrial Electronics**, IEEE, v. 66, n. 2, p. 1648–1656, 2019. Citado na página 18.

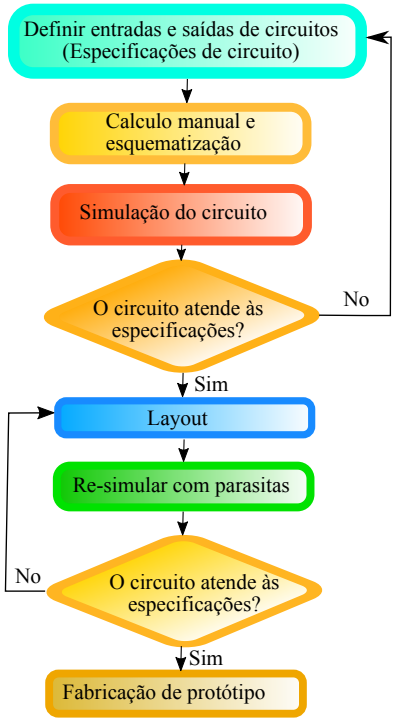
ZHAO, C. et al. A cmos on-chip temperature sensor with x2212;0.21 x00b0;c 0.17 x00b0;c inaccuracy from x2212;20 x00b0;c to 100 x00b0;c. In: **IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS2013)**. [S.l.: s.n.], 2013. p. 2621–2625. ISSN 0271-4302. Citado na página 60.

Apêndices

APÊNDICE A – FLUXOGRAMA PARA O PROCESSO DE *DESIGN* DO CI EM CMOS.

Nesta seção, apresenta-se o processo de *design* de CI em CMOS, junto com a metodologia e os resultados do trabalho de pesquisa. Como primeiro escopo explica-se o processo de *design* através de um fluxograma, como pode ser observado na Figura A.1. O processo tem como parâmetro inicial definir as entradas e saídas dos circuitos desejados, para continuar com um cálculo manual e projetar o esquemático, uma vez alcançado este ponto passa-se a simular o esquemático dos circuitos (simulação de *corners* e *Monte Carlo*), até que o circuito atenda às especificações requeridas. Seguidamente, desenvolve-se o *layout* de circuito, simulação *pós-layout* incluindo capacitâncias parasitas, e a reavaliação de entradas e saídas de circuito para sua fabricação.

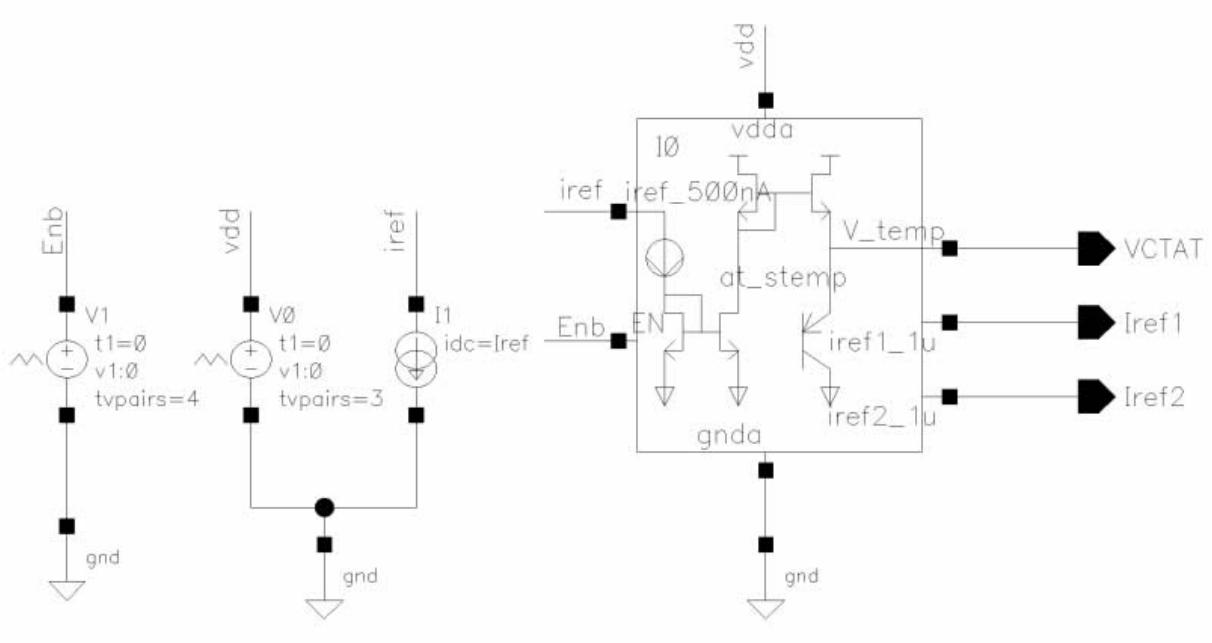
Figura A.1 – Fluxograma para o processo de *design* do CI em CMOS.



A metodologia seguida neste dissertação é baseado sobre o conceito de sistema-em-um-chip (*System-on-a-chip* - SoC). O sensor de resistência à adulteração (*Tamper resistance*) e o sensor de temperatura foram projetados em Cadence, empregando uma tecnologia padrão CMOS de 180 nm que opera com uma tensão de alimentação de 1,2 V. As simulações foram feitos na sequencia que mostra a Figura 3.1 simulando bloco por bloco.

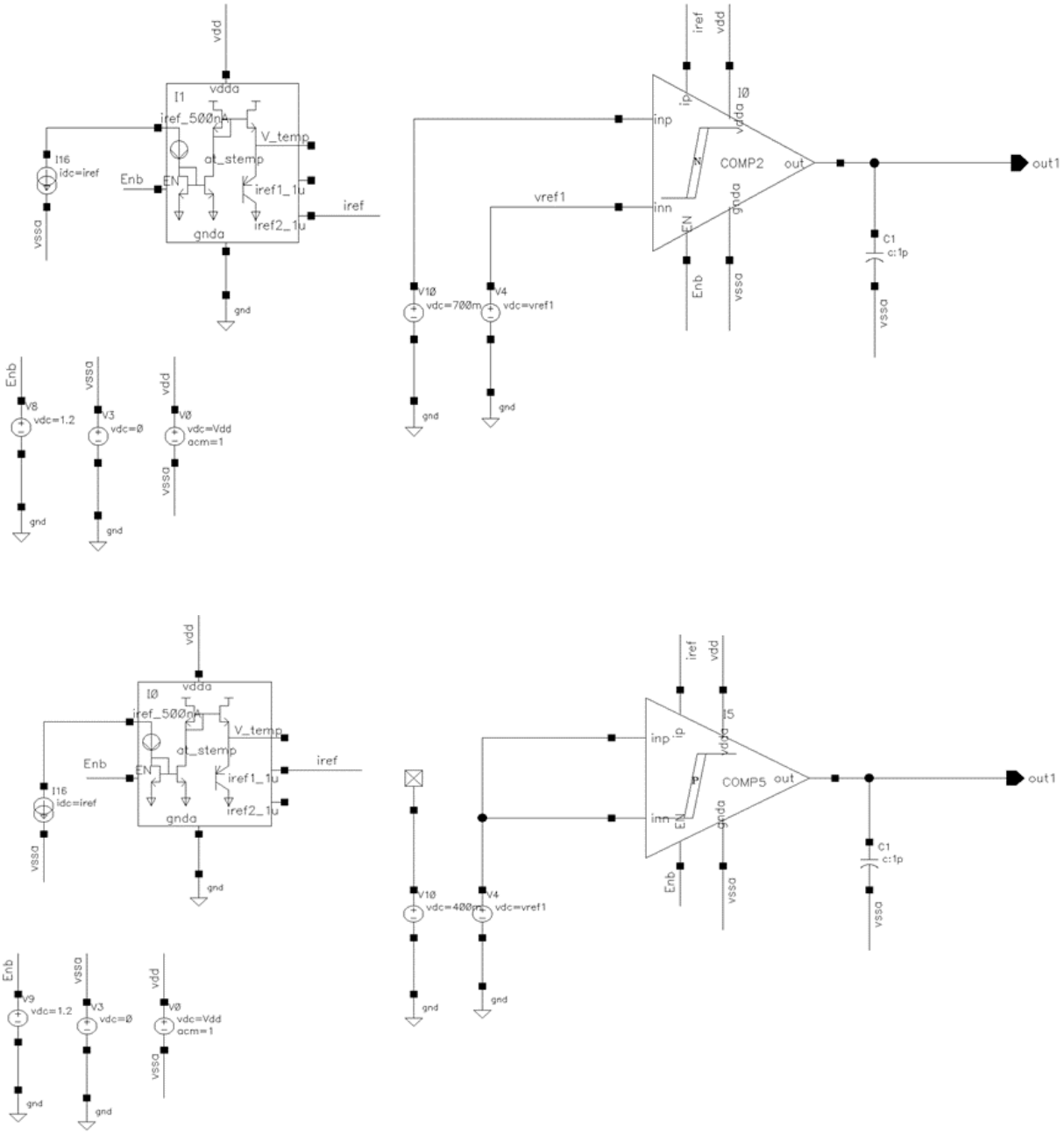
APÊNDICE B – CIRCUITOS DE SIMULAÇÃO DO SENSOR CTAT

Figura B.1 – Conexões necessárias para o teste de sensor CTAT.



APÊNDICE C – COMPARADOR DE PAR DIFERENCIAL TESTE

Figura C.1 – Configuração para o teste dos comparadores.



APÊNDICE D – SENSOR PROTETOR COMPLETO TESTE

Figura D.1 – Começões necessários para o teste de sensor protetor em temperatura de CI.