SIM-kaarti simuleeriv protsessorkaart *Gold Card* toorik.

Smart Card ehk maakeeli kiipkaart on sisuliselt väike arvuti koos oma operatsioonisüsteemi, failistruktuuri ja muu juurdekuuluvaga. Mida sellega teha saab?

SIM Salapärane ja muud protsessorkaardid

Kunagistel iidsetel aegadel, kui hakkasin ajakirja «Radio» lugema ja skeeme kokku tinutama, olid protsessorid üsna haruldased asjad. Isegi CMOS-mikroskeeme ei võetud niisama kätte, vaid püüti enne staatilisest laengust vabaneda, et kallid kivid otsi ei annaks. Mälupilt neist aegadest kujutab jupipoes nähtud eriti «ägedat» venda, kes sättis üht esimestest taskukalkulaatoritest rinnataskusse nii, et kõik seda võimalikult hästi näeksid.

Lisaks koopia tegemisele saab ühele SIM-kaardile kopeerida mitme operaatori info. Telefoni tekib lisamenüü, millest saate hetkel vajaliku operaatori valida ilma kaarte ringi tõstmata.

Nüüd keegi nende riistapuudega enam ei eputa – kontrollerid on igas võimalikus ja võimatus kohas. On vist aja küsimus, et ka WC-desse ilmuksid näpujälje ja/või silma iirise mustri skannerid. Keda süsteem ei tunne (= pole maksnud!), ajagu asju puu taga.

Loomulikult on kontrollerite kasutamine hea mõte, sest need on odavad ja keeruka skeemi saab kokku väga vähestest komponentidest, sest töökindlus on elektroonikas seda suurem, mida vähem on skeemis detaile – väiksem komponentide arv tähendab ka vähem potentsiaalselt halbu ühendusi. Rohkem kui 90% hädadest saab alguse just halbadest kontaktidest. Uskumatud Toomased kruvigu lahti oma kallis «Made in China» (PRC) kirjaga kodustereo ja vaadaku tähelepanelikult detailide jooteid. Või oleks siiski parem vaatamata jätta…

Üks koht, kus protsessoreid (või üldisemalt – kontrollereid) kasutatakse, on kiipkaardid. *Smart Card* ehk kiipkaart on sisuliselt väike arvuti koos oma operatsioonisüsteemi, failistruktuuri ja muu taolisega (ID kaart, telefonikaart).

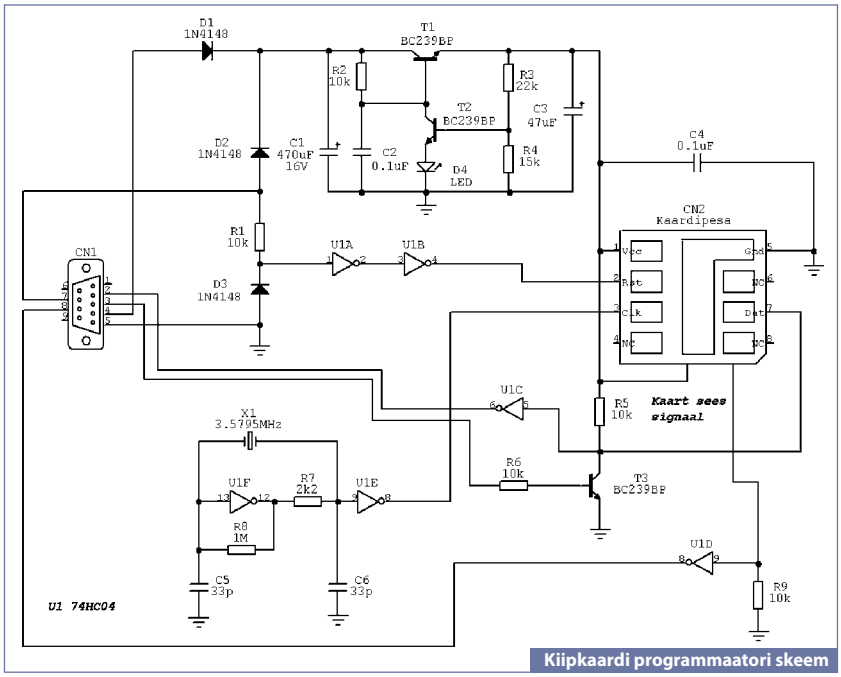
Mobiiltelefoni SIM-kaart (SIM – *subscriber identity module*) on samuti kiipkaart. Kui ID-kaardilt ei leia peale oma isikuandmete suurt midagi, siis SIM on juba tunduvalt huvitavam lugemisvara. Seal on telefoninumbrite kogum, mitmesugused turvavõtmed võrgu tarbeks jne. Kõike seda oleks huvitav analüüsida.

Paraku (või tegelikult – õnneks) on hulk infot krüpteeritud ja/või lihtsalt kättesaamatu. Mõnda asja annab siiski lugeda. Lisaks kõigele muule saab SIM-ist teha varukoopia. Selleks on vaja teist kaarti (*gold card*, *silver card* jne) ning programmaatorit. Viimase me seekord ehitamegi.

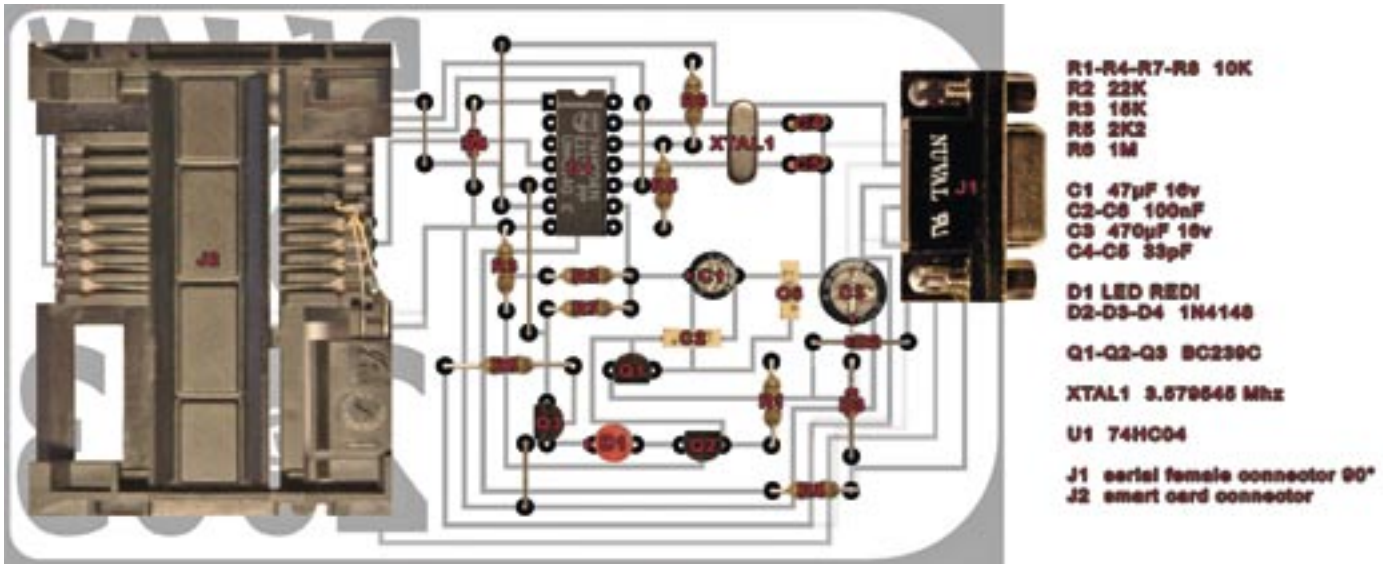
Dejan Kaljevici kiipkaardi lugeja/kirjutaja

Kiipkaartide programmaatorite skeeme leidub pea igal teisel võrgulehel. Originaallahendusi pakutakse aga vähe – enamasti kopeeritakse suure mobiiltelefoniguru Dejan Kaljevici lülitust. Skeem (vt joonist) on hästi lihtne ja sobib ehitamiseks ka elektroonikas veel mitte kodus olevatele lugejatele.

Lülitus sisaldab vaid hädavajalikke detaile, kõik tarbetud tuled–viled on siit välja visatud. Skeem ühendatakse arvuti järjestikporti. Toitepinge tuleb samast COM-pordist nn kvi-



Kiipkaardi programmaatori skeem



Kaardilugeja võimalik montaaživariant.

teerimissignaalide otstelt: viik 4 (DTR – *data terminal ready*) ja viik 7 (RTS – *ready to send*). Neid signaale kasutati arvutustehnika algusaegadel, kui perifeeriaseadmed (printer, modem vms) olid nii aeglased ja vähese puhvermäluga, et ei suutnud arvutist saadavat informatsiooni küllalt kiiresti töödelda.

Pordi otsad RTS ja DTR on väljundid. See tähendab, et viigule saab programmist lülitada +12 V või –12 V. Hea võimalus vähe voolu tarbivate (10 mA ja vähem) seadmete toitmiseks otse masinast. Elektri hind ju tõuseb pidevalt, ehk ongi hea lisatoiteploki arvelt kokku hoida.

Suurema voolu saamiseks liidetakse RTS ja DTR väljundite pinged üle dioodide D1 ja D2 kokku. Nii ei koormata porti, kui selle viik RTS on näiteks tasemel +12 V ja DTR pingel –12 V. Lisaks sellele ei lase dioodid skeemi miinuspinget (kui kaardilugemisprogramm veel ei tööta).

Lülitus elementidel T1, T2, R2…R4, D4, C2 ja C3 stabiliseerib pordist võetud pinge +5 V-le. Pinge võib ju kõikuda ja koormuse muutumisel (lugemine, kirjutamine) muutub kindlasti. Kaart tahab stabiilset pinget.

Punane valgusdiood D4 pole niisama iluasi, vaid nn tugipinge allikas. Põlevale dioodile jääb umbes 1,6 V. Sellega juhitakse regulaatori transistori T1. Väljundpinge saab täpselt paika seada, muutes takistit R4 või R3.

Muide, kuna sinisel valgusdioodil on pinge tunduvalt kõrgem (>2,6 V), ei sobi see seekord skeemi.

SIM-kaarti on lugemis-/kirjutamisoperatsioonide kestel vaja mõnikord nullida. Selleks on tal viik RST (*restart*), mida juhitakse samuti pordi kaudu. Kuna nullimise impulss võib olla lühike, kasutatakse ära toiteviik. Enamiku ajast hoitakse signaali RTS-i tasemel +12 V ja see toidab skeemi. Vajadusel lülitatakse see korraks –12 V-le ja siis tagasi. Kaart saab nullitud, aga skeemi toitega ei juhtu midagi, sest piisavalt suure mahtuvusega konde C1 ei lase pingel liiga palju langeda. Nutikas lahendus!

Skeemis on puhvritena kasutatud loogikakivi 74HC04. Sellise mikroskeemi toitepinge ja ka maksimaalne sisendpinge on +5 V. Pordi viigu RTS kaudu tulevat +/-12 V juhtsignaali konditsioneerib ahel R1,D3. Esimene neist piirab voolu ja teine ei lase miinuspinget peale (piirab -0,6 V-le, mis on kahjutu). Üle +5 V pinge kivil minna ei saa: selle eest hoolitsevad «satika» sees asuvad sisendilt toitesse minevad kaitsedioodid. Nullimisahelas on kaks puhvrit. Esimene neist on seotud pingetasemete sobitamisega ja teine keerab signaali tagasi õigele «polaarsusele» (on ju elemendid U1A ja U1B mõlemad inverterid, mis tähendab, et väljundtase on täpselt vastupidine sisendtasemele).

Kõik kontrollerid vajavad tööks taktsignaaligeneraatorit. Mida kiirem on takt, seda kiiremini arvuti (kontroller) oma ülesandeid täidab. Kaart on õhuke plastiliistakas, mida tihti painutatakse. Seega sinna kvartskristalli hästi ei topi. Kasutatakse välist generaatorit. Meie skeemis on see realiseeritud kivi U1 elemendil F. Takistiga R8 viiakse tavaliselt nulle ja ühtesid seediv skeem võimendusrežiimi, kus pinge sisendis ja väljundis on umbes pool toitepingest. Positiivne tagasiside kvartsi X1 kaudu sunnib skeemi võnkuma ainult kvartsile märgitud sagedusel. Väikese mahtuvusega konded C5 ja C6 pole ilmtingimata vajalikud, kuid nad kergendavad generaatori võnkumahakkamist. Mõnel juhul võib skeem töötada ka ilma nendeta. Mikroskeemi U1 element E töötab lihtsalt puhvrina (vahevõimendi), mis ei lase kaardil generaatorit «välja suretada». Lisaks teeb ta generaatori «ebamäärasest» võnkumisest korraliku nelinurksignaali.

Protsessorkaart suhtleb laia maailmaga üheainsa andmesideviigu kaudu. Seda mööda loetakse kord käske ja siis jälle väljastatakse andmeid. Kuna järjestikpordil on eraldi saate- ja vastuvõtuotsad, tuleb signaalid kuidagi kokku liita. Selleks on skeemis ahel R6, T3

(masinast tulev andmevoog kaardile) ja U1 element C (andmekaardilt arvutisse). Signaalid summeeruvad ühisel koormustakistil R5. Miks need segamini ei lähe? Sellepärast, et saade ja vastuvõtt toimuvad erineval ajal.

Kondensaatorid C3 ja C4 siluvad skeemi toitepinget, kusjuures viimane šunteerib impulsshäireid, mis loogikalülitusi sisaldavates skeemides alati tekivad. Sellise otstarbega kondensaatorit nimetatakse lahtisidestuskondeks ja neid on soovitatav panna lausa iga loogikaelemendi toiteviikudele (võimalikult mikroskeemi lähedale). Antud skeemis on U1 toiteviigud 7 (maa) ja 14 (+5 V).

Ja lõpuks – takisti R9 ja mikroskeemi U1 elemendi D kaudu antakse programmile teada, et kiipkaart on lugejas.

Detailid ja häälestamine

Nagu ikka, olen püüdnud vältida skeemis eksootilisi, kalleid ja raskesti kättesaadavaid komponente. Kõik jupid on «tavalised», neid leiab igast elektroonikapoest. Sobivad ¼ W võimsusega takistid ja laiatarbekondensaatorid. Ainult C1 peab kannatama vähemalt 16 V, teiste kondede tööpinge võib olla veelgi madalam.

Kui skeemi toitepinget ei õnnestu kuidagi +5 V-ni viia, tuleb 1N4148-tüüpi dioodid asendada sellistega, millel madalam pingekadu, näiteks Šhottky dioodidega 1N5819.

Meie skeemi kõige keerukam element on kiipkaardi pesa. Õnneks saab ka neid poest vabalt osta, hinda on tükil natuke üle 20 raha. Kui aga peale supermarketite ühtki asjalikku ostukohta läheduses pole, saab pesa ka ise ehitada. Variante on mitu – jupp trükkplaati koos vanast testrist «laenatud» painduvate klemmidega, plastkarbi sisse sulatatud vedrutraadi tükid või isegi arvuti emaplaadilt võetud PCI-siinipesa. Viimasesse tuleb lihtsalt pilu saagida ja liigsed klemmid eemaldada. Selline lahendus töötas üsna edukalt.

Kogu lülituse saab monteerida ühepoolsele trükkplaadile. Montaažijoonise ühe variandi leiate näiteks aadressilt *www.elektroda.pl/dla_kompa/dejan/components.jpg*.

Kui skeem on kokku pandud, tuleks seda ettevaatuse mõttes kõigepealt testida. Ühendame lülituse arvuti COM-pordiga ja käivitame Hyperterminali. Pinged pordi otstel DTR (4) ja RTS (7) on +12 V või moodsates masinates natuke vähem. LED D4 süttib. Mõõdame pinget kondensaatoril C3 – see peab olema +5 V. Vajadusel saab pinget reguleerida takisti R4 väärtust muutes.

Järgnevalt katsetame andmesignaalide ahelate korrasolekut. Toksides klaviatuurilt testfraasi «suur reheahi», peab see samal kujul ekraanile ilmuma. Kui ilmub, on skeem korras.

Jääb veel veenduda generaatoriosa töötamises. Selleks on vaja ostsilloskoobi-nimelist vigurit, sest tavalise

multimeetriga ei saa 3,5M Hz võnkumiste olemasolu kuidagi tuvastada. Sagedusmõõtja sobib ka. Vajalike mõõteriistade puudumisel jääb vaid loota, et skeem töötab.

Kui generaator ei taha miskipärast võnkuda, võib püüda veidi muuta takisti R8 väärtust või lülitada lahti üks (või mõlemad) kondensaatoritest C5/C6. Edasi pistame programmaatorisse mõne tarbetu SIM-kaardi ja hakkame katsetama.

Tarkvara

Võrguavarustes leidub SIM-kaartide häkkimiseks erinevat softi lausa gigabaitide kaupa. Üks laiemalt levinud programmidest on Dejan SimScan. Seda ja hulka muud hääd softi saab sikutada näiteks naabrite juurest aadressilt *www.unlock.lv*, samuti saidilt *www.mfgware.com*.

Kvarts sagedusel 3,5795 MHz.

Kasulikku teavet SIM-kaartide, nendest varukoopiate tegemise ja SimScani kasutamise kohta leiate netiaadressilt *www.kievsat.com/gsm/index.htm#progr*. Selgub, et Dejan SimScan on mõeldud põhiliselt kaardi peidetud võtmete «Ki» ja «IMSI» väljanuhkimiseks. Miks seda vaja on? Nii saab teha kaardist näiteks varukoopia. Asjad kipuvad ju ikka kaduma või rikki minema. Heakene küll, uue kaardi saab ka telefonifirmalt, kuid teie telefoniraamatut ei taasta enam keegi. Koopia tehakse SIM-kaarti simuleerivale protsessorkaardile – Gold Card, Silver Card, FunCard jms, mis satelliidituuneritega tegelejatele hästi tuttavad.

Kiipkaardi programmaatori detailide loetelu

Komponent	Pos. nr.	Nominaal	Kogus
Kondensaator	C1	470uF/16V	1
	C3	47 uF	1
	C2,C4	100 nF	2
	C5,C6	33 pF	2
Mikroskeem	U1	74HC04	1
Transistor	T1...T3	BC239C	3
LED	D4	punane	1
Diood	D1…D3	1N4148	3
Takisti	R1,R2,R5,R6,R9	10k	5
	R3	22k	1
	R4	15k	1
	R7	2,2k	1
	R8	1M	1
Pistik	CN1	DB9F	1
	CN2	kaardipesa	1
Kvarts	X1	3,5795 MHz	1

Mis imeriistad need kuld-, hõbe- jms kaardid siis on? Selgub, et ei midagi erilist: lihtsalt ISO7816 standardile vastava kontaktistikuga kaardid, mis sisaldavad Microchip PIC või Atmeli protsessorit. Lisaks on kaardil nn E2PROM mälu. Ongi kõik! Erinevad asenduskaardid on erinevate mälumahtudega ja protsessoritega. Põhjalikuma ülevaate saab lehelt *www.flycont.com/lab/labmenu/chip_card/chip_card.html*. Sealt selgub, et näiteks satimeeste üks lemmikutest – *FunCard* – sisaldab protsessorit AT90S8515A ja mälu 24LC256, kuldkaardis aga on peidus vana sõber PIC16F84!

Enne programmi kasutamist lugege hoolikalt eespool nimetatud võrgulehte (vene keeles!), sest teatud tüüpi SIM-kaardid lähevad häkkimise käigus lukku. Selle vältimiseks peab nn A38 piiranguväljas olev arv olema väiksem kui 64000.

Lisaks kõigele muule saaks kuldkaardist (ja analoogsetest) teha midagi asjalikku – kas või koduse valvesüsteemi võtme. Parem igatahes, kui taevakanalilt raske raha eest muretsetud legaalse kaardiga rämpsreklaame vaadata. Aga noh, maitse asi.

Kas lülituse iseehitamine tuleb odavam, kui poest valmis seade osta? Paistab küll. Nägin üht analoogset, kuid veidi keerukama skeemiga lülitust poeletil. Hinnasilt teatas: 690 krooni! Selle kullahinnaga seadme skeemi leiate võrguaadressilt *www.irda.ru/photo/cables/unibox/USIv20.htm#1*. Samas leidub veel hulk soovitusi tööks (SIM-)kaartidega. Kuna veebileht kasutab vene fonte, tuleb brauseris lülitada sisse kirillitsakodeering.

Kui juba kiipkaartidega ja nende protsessoritega tegelda, tasuks ehk ehitada veelgi universaalsem programmaator. Lehel *www.kievsat.com/programmat/index.htm* kujutatud seade lubab lisaks kirjutada ka mitmeid protsessoreid ja E2PROM-mälusid. Skeemid ja soft asuvad samal lehel.

Pidage siis meeles, et piraatlus on rangelt keelatud… ja katsetage alati enne mingi sellise kaardiga, mille riknemisest või lukkuminekust kahju pole.

Head häkkimist!

felc@edu.ttu.ee