Fişa suspiciunii de plagiat / Sheet of plagiarism's suspicion	Indexat la: 32/06

Opera suspicionată (OS) Suspicious work	Opera autentică (OA) Authentic work

OS	Mang I., "Considerations on hardware implementations of encryption algorithms", *Visnik Sumskovo derjavnovo universitety, Seria Technichni nauki* 12(71), p.41-50, 2004 Disponibil la: http :// essuir . sumdu . edu . ua / handle / 123456789 / 10536.
OA	Elbirt, A.J., Yip,W., Chetwynd, B., Paar, C., „An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algoritm Finalists", The Third Advance Encryption Standard (AES3) Candidate Conference, New York, April 13-14, 2000. Disponibil la: http :// www . ei . rub . de / media / crypto / veroeffentlichungen / 2011 / 01 / 21 / aelbirtetalaes3 . pdf

Incidența minimă a suspiciunii / Minimum incidence of suspicion	
p.41:6 – p.41:17	p.1:24 – p.2:7
p.41:31 – p.42:36	p.3:5 – p3:28
p.43:Table 1	p.5:Table 1

An FPGA Im lement ti n n Perf rm nce Ev lu ti n f the AES Bl ck Ci her C n i te Al rithm Fin lists *

AJ Elbirt[1], W Yi [1], B Chetwyn [2], C Paar[1]
Electrical an C m uter Engineering De artment
W rce ter P lytechnic In titute
100 In titute R a , W rce ter, MA 01609, USA

[1] Email: aelbirt, waihyi , christ f @ece.w i.e u
[2] Email: s unge@alum.w i.e u

The Thi A vance Enc y tion Stan a (AES3) Can i ate Confe ence,
A il 13-14, 2000, New Yo k, USA.

A str ct

The technical analysis use in etermining which f the A vance Encry ti n tan ar can i ates will be selecte as the A vance Encry ti n Alg rithm inclu es efficiency testing f b th har ware an s ftware im lementati ns f can i ate alg rithms. Re r grammable evices such as Fiel Pr grammable Gate Arrays (FPGAs) are highly attractive ti ns f r har ware im lementati ns f encry ti n alg - rithms as they r vi e cry t gra hic alg rithm agility, hysical security, an tentially much higher erf rmance than s ftware s luti ns. This c ntributi n investigates the significance f FPGA im lementati ns f f ur f the A vance Encry ti n tan ar can i ate alg rithm finalists. Multi le architectural im lementati n ti ns are ex l re f r each alg rithm. A str ng f cus is lace n high thr ugh ut im lementati ns, which are require t su rt security f r current an future high ban wi th a li- cati ns. The im lementati ns f each alg rithm will be c m are in an eff rt t etermine the m st suitable can i ate f r har ware im lementati n within c mmercially available FPGAs.

Keyw r s: cry t gra hy, alg rithm-agility, FPGA, l ck ci her, VHDL

1 Intr ucti n

The Nati nal Institute f tan ar s an Techn l gy (NI T) has initiate a r cess t evel a Fe eral Inf r- mati n Pr cessing tan ar (FIP) f r the A vance Encry ti n tan ar (AE), s ecifying an A vance Encry ti n Alg rithm t re lace the Data Encry ti n tan ar (DE) which ex ire in 1 8 [1]. NI T has s licite can i ate alg rithms f r inclusi n in AE , resulting in fifteen fficial can i ate alg rithms f which five have een selecte as finalists. Unlike DE , which was esigne s ecifically f r har ware im lementa- ti ns, ne f the esign criteria f r AE can i ate alg rithms is that they can e efficiently im lemente in th har ware an s ftware. Thus, NI T has ann unce that th har ware an s ftware erf rmance mea- surements will e inclu e in their efficiency testing. far, h wever, virtually all erf rmance c m aris ns have een restricte t s ftware im lementati ns n vari us latf rms [2].

*This research was su orte in art through NSF CAREER awar #CCR-9733246.

The a vantages f a s ftware im lementati n inclu e ease f use, ease f u gra e, rta ility, an flexi ility. H wever, a s ftware im lementati n ffers nly limite hysical security, es ecially with res ect t key st rage [3] [4]. C nversely, cry t gra hic alg rithms (an their ass ciate keys) that are im lemente in har ware are, y nature, m re hysically secure as they cann t easily e rea r m ifie y an utsi e attacker [4]. The wnsi e f tra iti nal (A IC) har ware im lementati n are the lack f flexi ility with res ect t alg rithm an arameter switch. A r mising alternative f r im lementati n l ck ci her are rec nfigura le har ware evices such as Fiel Pr gramma le Gate Arrays (FPGAs). FPGAs are har ware evices wh se functi n is n t fixe an which can e r gramme in-system. The tential a vantages f encry ti n alg rithms im lemente in FPGAs inclu e:

Alg rithm Agility This term refers t the switching f cry t gra hic alg rithms uring erati n. The maj rity f m ern security r t c ls, such as L r IPsec, all w f r multi le encry ti n alg - rithms. The encry ti n alg rithm is neg tiate n a er-sessi n asis; e.g., IPsec all ws am ng thers DE , 3DE , Bl wfish, CA T, IDEA, RC4 an RC6 as alg rithms, an future extensi ns are ssi le. Whereas alg rithm agility is c stly with tra iti nal har ware, FPGAs can e re r gramme n-the-fly.

Alg rithm U l a It is erceiva le that fiel e evices are u gra e with a new encry ti n alg rithm which i n t exist (r was n t stan ar ize !) at esign time. In articular, it is very attractive f r numer us security r ucts t e u gra e f r use f AE nce the selecti n r cess is ver. Assuming there is s me kin f (tem rary) c nnecti n t a netw rk such as the Internet, FPGA-equi e encry ti n evices can u l a the new c nfigurati n c e.

Alg rithm M ificati n There are a licati ns which require m ificati n f a stan ar ize alg rithm, e.g., y using r rietary - xes r ermutati ns. uch m ificati ns are easily ma e with rec nfigura le har ware. imilarly, a stan ar ize alg rithm can e swa e with a r rietary ne. Als , m es f erati n can e easily change .

Architecture Efficiency In certain cases, a har ware architecture can e much m re m re efficient if it is esigne f r a s ecific set f arameters; e.g., c nstant multi licati n (f integers r in Gal is fiel s) is far m re efficient than general multi licati n. With FPGAs it is ssi le t esign an timize an architecture f r a s ecific arameter set.

Thr ugh ut Alth ugh ty ically sl wer than an A IC im lementati ns, FPGA im lementati ns have the tential f running su stantially faster then s ftware im lementati ns.

C st Efficiency The time an c sts f r evel ing an FPGA im lementati n f a given alg rithm are much l wer than f r an A IC im lementati n. (H wever, f r high-v lume a licati ns, A IC s luti ns usually ec me the m re c st-efficient ch ice.)

N te that alg rithm agility remains an en research issue in regar s t s ee , hysical security, an the c st ass ciate with current high-en FPGA evices. H wever, we elieve that c st is n t a l ng-term limiting fact r, as will e iscusse in ecti n 3.3. F r these reas ns, this a er escri es a th r ugh c m aris n the AE finalist alg rithms RC6, Rijn ael, er ent, an Tw fish with res ect t im lementati n n state- f-the-art FPGAs. ne as ect that seems t e es ecially relevant is the investigati n f achieva le encry ti n rates f r FPGA- ase im lementati ns. We em nstrate that FPGA s luti ns encry t at rates in the Giga it range f r all f ur alg rithms investigate , which is at least ne r er f magnitu e faster than m st re rte s ftware im lementati ns [ ].

What f ll ws is an investigati n f the AE finalists t etermine the nature f their un erlying c m-nents. The characterizati n f the alg rithms' c m nents will lea t a iscussi n f the har ware architectures est suite f r im lementati n f the AE finalists. A erf rmance metric t measure the har ware c st f r the thr ugh ut achieve y each alg rithm's im lementati ns will e evel e an a

target FPGA will e ch sen s as t yiel im lementati ns that are timize f r high-thr ugh ut era-ti n within the c mmercially availa le evice. Finally, multi le architecture ti ns f the alg rithms within the targete FPGA will e iscusse an the verall erf rmance f the im lementati ns will e evaluate versus ty ical s ftware im lementati ns.

2 Previ us W rk

As se t cust m har ware r s ftware im lementati ns, little w rk exists in the area f l ck ci her im lementati ns within existing FPGAs. DE , the m st c mm n l ck ci her im lementati n targete t FPGAs, has een sh wn t erate at s ee s f u t 400 M it/s [6]. We elieve that this erf rmance can e greatly enhance using t ay's techn l gy. These s ee s are significantly faster than the est s ftware im lementati ns f DE [7] [8] [ ], which ty ically have thr ugh uts el w 100 M it/s, alth ugh a 137 M it/s im lementati n has een re rte as well [7]. This erf rmance ifferential is an ex ecte result f DE having een esigne in the l 70s with har ware im lementati ns in min .

ther l ck ci hers have een im lemente in FPGAs with varying egrees f success. A ty ical exam-le is the IDEA l ck ci her which has een im lemente at s ee s ranging fr m 2.8 M it/s [10] t 28 M it/s [11]. N te that while the 28 M it/s thr ugh ut was achieve in a fully i eline architecture, the im lementati n require f ur Xilinx XC4000 FPGAs.

me FPGA im lementati n thr ugh uts f r the AE can i ates have een sh wn t e far sl wer than their s ftware c unter arts. Har ware thr ugh uts f a ut 12 M it/s [12] [13] have een achieve f r CA T-2 6. H wever, s ftware im lementati ns have resulte in thr ugh uts f 37.8 M it/s f r CA T-2 6 n a 200 MHz PentiumPr PC [ ], a fact r f three faster than FPGA im lementati ns. When scale t a m re current 600 MHz PentiumPr PC, it is ex ecte that the same s ftware im lementati n w ul ut erf rm FPGA im lementati ns y an even larger fact r. While an FPGA im lementati n f RC6 achieve ata rates f 37.8 M it/s [13], ur fin ings in icate that c nsi era ly higher ata rates are achieva le.

When examining the AE finalists, it is im rtant t n te that they n t necessarily exhi it similar ehavi r t DE when c m aring har ware an s ftware im lementati ns. ne reas n f r this is that the AE finalists have een esigne with efficient s ftware im lementati ns in min . A iti nally, s ftware im lementati ns may e execute n r cess rs erating at frequencies as high as 800 MHz while ty ical im lementati ns that target FPGAs reach a maximum cl ck frequency f 0 MHz.

3 Meth l gy

3.1 Design Meth l gy

There are tw asic har ware esign meth l gies currently availa le: language ase (high level) esign an schematic ase (l w level) esign. Language ase esign relies u n synthesis t ls t im lement the esire har ware. While synthesis t ls c ntinue t im r ve, they rarely achieve the m st timize im lementati n in terms f th area an s ee when c m are t a schematic im lementati n. As a result, synthesize esigns ten t e (slightly) larger an sl wer than their schematic ase c unter arts. A iti nally, im lementati n results can greatly vary e en ing n the synthesis t l as well as the esign eing synthesize , lea ing t tentially increase variances in the synthesize results when c m aring synthesis t l ut uts. This situati n is n t entirely ifferent fr m a s ftware im lementati n f an alg rithm in a high-level language such as C, which is als e en ent n c ing style an c m iler quality. As sh wn in [14], schematic ase esign meth l gies are n l nger feasi le f r su rting the increase in architectural c m lexity evi ence y m ern FPGAs. As a result, a language ase esign meth l gy was ch sen as the im lementati n f rm f r the AE finalists with VHDL eing the s ecific language ch sen.

3.2 Im lement ti ns — Gener l C nsi er ti ns

Each AE finalist was im lemente in VHDL using a tt m-u esign an test meth l gy. The same har ware interface was use f r each f the im lementati ns. In an eff rt t achieve the maximum efficiency ssi le, n te that key sche uling an ecry ti n were n t im lemente f r each f the AE finalists. Because FPGAs may e rec nfigure in-system, the FPGA may e c nfigure f r key sche uling an then later rec nfigure f r either encry ti n r ecry ti n. This ti n is a maj r a vantage f FPGAs im lementati ns ver classical A IC im lementati ns. R un keys f r encry ti n are l a e fr m the external key us an are st re in internal registers an all keys must e l a e ef re encry ti n may egin. Key l a ing is isa le until encry ti n is c m lete . Each im lementati n was simulate f r functi nal c rrectness using the test vect rs r vi e in the AE su missi n ackage [1] [16] [17] [18]. After verifying the functi nality f the im lementati ns, the VHDL c e was synthesize , lace an r ute , an re-simulate with ann tate timing using the same test vect rs, verifying that the im lementati ns were successful.

3.3 Selecti n f T rget FPGA

When examining the AE finalists f r har ware im lementati n within an FPGA, a num er f key as ects emerge. First, it is vi us that the im lementati n will require a large am unt f I/ ins t fully su rt the 128- it ata stream at high s ee s where us multi lexing is n t an ti n. It is esira le t ec u le the 128- it in ut an ut ut ata streams t all w f r a fully i eline architecture. ince the r un keys cann t change uring the encry ti n r cess, they may e l a e via a se arate key in ut us ri r t the start f encry ti n. A iti nally, t im lement a fully i eline architecture requires 128- it wi e i eline stages, resulting in the nee f r a register-rich architecture t achieve a fast, synchr n us im lementati n. M re ver, it is esira le t have as many register its as ssi le er each f the FPGA's c nfigura le units t all w f r a regular lay ut f esign elements as well as t minimize the r uting require etween c nfigura le units. Finally, it is critical that fast carry-chaining e r vi e etween the FPGA's c nfigura le units t maximize the erf rmance f AE finalists that utilize arithmetic erati ns [13] [12].

In a iti n t architectural requirements, scala ility an c st must e c nsi ere . We elieve that the ch sen FPGA sh ul e the est chi availa le, ca a le f r vi ing the largest am unt f har ware res urces as well as eing highly flexi le s as t yiel timal erf rmance. Unf rtunately, the c st ass ciate with current high-en FPGAs is relatively high (several hun re U llars er evice). H wever, it is im rtant t n te that the FPGA market has hist rically ev lve at an extremely ra i ace, with larger an faster evices eing release t in ustry at a c nstant rate. This ev luti n has resulte in FPGA c st-curves that ecrease shar ly ver relatively sh rt eri s f time. Hence, selecting a high-en evice r vi es the cl sest m el f r the ty ical FPGA that will e availa le ver the ex ecte lifes an f AE .

Base n the af rementi ne c nsi erati ns, the Xilinx Virtex XCV1000BG 60-4 FPGA was ch sen as the target evice. The XCV1000 has 128K its f em e e RAM ivi e am ng thirty-tw RAM l cks that are se arate fr m the main y f the FPGA. The 60- in all gri array ackage r vi es 12 usa le I/ ins. The XCV1000 is c m rise f a 64 × 6 array f l k-u -ta le ase C nfigura le L gic Bl cks (CLBs), each f which acts as a 4- it element c m rise f tw 2- it slices f r a t tal f 12288 CLB slices [1]. This ty e f c nfigurati n results in a highly flexi le architecture that will acc mm ate the r un functi ns' use f wi e eran functi ns. N te that the XCV1000 als a ears t e a g re resentative f r a m ern FPGA an that evices fr m ther ven rs are n t fun amentally ifferent. It is thus h e that ur results carry ver, within limits, t ther evices.

3.4 Design T ls

FPGA Ex ress y yn sys, Inc. an yn lify y yn licity, Inc. were use t synthesize the VHDL im lementati ns f the AE finalists. As this stu y laces a str ng f cus n high thr ugh ut im lementati ns,

the synthesis t ls were set t timize f r s ee . As will e iscusse in ecti n 6, the resultant im lementati ns exhi it the est ssi le thr ugh uts with the ass ciate c st eing an increase in the area require in the FPGA f r each f the im lementati ns. imilarly, if the synthesis t ls were set t timize f r area, the resultant im lementati ns w ul exhi it re uce area requirements at the c st f ecrease thr ugh ut.

XACTste 2.1i y Xilinx, Inc. was use t lace an r ute the synthesize im lementati ns. F r the su - i eline architectures, a 40 MHz timing c nstraint was use in th the synthesis an lace-an - r ute r cesses as it resulte in significantly higher system cl ck frequencies. H wever, the 40 MHz timing c nstraint was f un t have little affect n the ther architecture ty es, resulting in nearly i entical system cl ck frequencies t th se achieve with ut the timing c nstraint.

Finally, ee wave y Viewl gic ystems, Inc. an Active-HDL^{TM} y ALDEC, Inc. were use t erf rm ehavi ral an timing simulati ns f r the im lementati ns f the AE finalists. The simulati ns verifie th the functi nality an the a ility t erate at the esignate cl ck frequencies f r the im lementati ns.

4 Architecture ti ns n the AES Fin lists

Bef re attem ting t im lement the AE finalists in har ware, it is im rtant t un erstan the nature f each alg rithm as well as the har ware architectures m st suite f r their im lementati n. What f ll ws is an investigati n int the key c m nents f the AE finalists. Base n this reak wn, a iscussi n is resente n the har ware architectures m st suite f r im lementati n f the AE finalists.

4.1 C re er ti ns f the AES Fin list Alg rithms

Alg rithm	X R	M 2^{32} A	M 2^{32} Su tr ct	Fixe Shift	V ri le R t te	M 2^{32} Multi ly	GF(2^8) Multi ly	LUT
MAR	•	•	•	•	•	•		•
RC6	•	•		•	•	•		
Rijn ael	•			•			•	•
er ent	•			•				•
Tw fish	•	•		•			•	•

Ta le 1: AE finalists c re erati ns [20]

M ern FPGAs have a structure c m rise f a tw - imensi nal array f c nfigura le functi n units interc nnecte via h riz ntal an vertical r uting channels. C nfigura le functi n units are ty ically c m- rise f l k-u -ta les an fli -fl s. L k-u -ta les may e c nfigure as either c m inati nal l gic r mem ry elements. A iti nally, many m ern FPGAs r vi e varia le-size RAM l cks that may e use as either mem ry elements r l k-u -ta les [21].

In terms f c m lexity, the erati ns etaile in Ta le 1 that require the m st har ware res urces as well as c m utati n time are the m ul 2^{32} multi licati n an the varia le r tati n erati ns [20]. Im lementing wi e multi liers in har ware is an inherently ifficult task that requires significant har ware res urces. A iti nally, alg rithms that em l y large varia le r tati ns require a m erate am unt f multi lexing har ware if carefully esigne (see ecti n .1 f r further iscussi n). -B xes may e im lemente in either c m inat rial l gic r em e e RAM — the a vantages f each f these ti ns are iscusse in ecti n 4.2. Fast erati ns such as it-wise X R, m ul 2^{32} a iti n an su tracti n, an fixe value shifting are c n- structe fr m sim le har ware elements. A iti nally, the Gal is fiel multi licati ns require in Rijn ael an Tw fish can als e im lemente very efficiently in har ware as they are multi licati ns y a c nstant. Gal is fiel c nstant multi licati n requires far less res urces than general multi licati ns [22].

Base n ur evaluati n f the AE finalists, the MAR alg rithm a eare t e the m st res urce intensive ase n its use f large -B xes, an m ul 2^{32} multi licati n. As a result, it was c njecture

that the MAR alg rithm w ul exhi it lesser erf rmance when c m are t the ther AE finalists. Due t this evaluati n an a lack f evel ment res urces, the MAR alg rithm was mitte fr m this stu y.

4.2 H r w re Architectures

The AE finalists are all c m rise f a asic l ing structure (s me f rm f either Feistel r su stituti n-ermutati n netw rk) where y ata is iteratively asse thr ugh a r un functi n. Base n this l ing structure, the f ll wing architecture ti ns were investigate s as t yiel timize im lementati ns:

- Iterative L ing
- L Unr lling
- Partial Pi elining
- Partial Pi elining with u -Pi elining

Iterative l ing ver a ci her's r un structure is an effective meth f r minimizing the har ware require when im lementing an iterative architecture. When nly ne r un is im lemente , an n-r un ci her must iterate n times t erf rm an encry ti n. This a r ach has a l w register-t -register elay ut a requires a large num er f cl ck cycles t erf rm an encry ti n. This a r ach als minimizes in general the har ware require f r r un functi n im lementati n ut can e c stly with res ect t the har ware require f r r un key an -B x multi lexing. Iterative l ing is a su set f l unr lling in that nly ne r un is unr lle whereas a l unr lling architecture all ws f r the unr lling f multi le r un s, u t the t tal num er f r un s require y the ci her. As se t an iterative l ing architecture, a l unr lling architecture where all n r un s are unr lle an im lemente as a single c m inat rial l gic l ck maximizes the har ware require f r r un functi n im lementati n while the har ware require f r r un key an -B x multi lexing is c m letely eliminate . H wever, while this a r ach minimizes the num er f cl ck cycles require t erf rm an encry ti n, it maximizes the w rst case register-t -register elay f r the system, resulting in an extremely sl w system cl ck.

A artially i eline architecture ffers the a vantage f high thr ugh ut rates y increasing the num er f l cks f ata that are eing simultane usly erate u n. This is achieve y re licating the r un functi n har ware an registering the interme iate ata etween r un s. M re ver, in the case f a full-length i eline (a s ecific f rm f a artial i eline), the system will ut ut a 128- it l ck f ci hertext at each cl ck cycle nce the latency f the i eline has een met. H wever, an architecture f this f rm requires significantly m re har ware res urces as c m are t a l unr lling architecture. In a artially i eline architecture, each r un is im lemente as the i eline's at mic unit an are se arate y the registers that f rm the actual i eline. H wever, many f the AE finalists cann t e im lemente using a full-length i eline ue t the large size f their ass ciate r un functi n an -B xes, th f which must e re licate n times f r an n-r un ci her. As such, these alg rithms must e im lemente as artial i elines. A iti nally, a i eline architecture can e fully ex l ite nly in m es f erati ns which n t require fee ack f the encry te ata, such as Electr nic C e-B k r C unter M e [3, ecti n .]. When erating in fee ack m es such as Ci hertext Fee ack M e, the ci hertext f ne l ck must e availa le ef re the next l ck can e encry te . As a result, multi le l cks f laintext cann t e encry te in a i eline fashi n when erating in fee ack m es. F r the remain er f ur iscussi n, fee ack m e will e a reviate as FB an n n-fee ack m e will e a reviate as NFB.

u - i elining a (artially) i eline architecture is a vantage us when the r un functi n f the i eline architecture is c m lex, resulting in a large elay etween i eline stages. By a ing su - i eline stages, the at mic functi n f each i eline stage is su - ivi e int smaller functi nal l cks. This results in a ecrease in the i eline's elay etween stages. H wever, each su - ivisi n f the at mic functi n increases the num er f cl ck cycles require t erf rm an encry ti n y a fact r equal t the num er f

su - ivisi ns. At the same time, the num er f l cks f ata that may e erate u n in NFB m e is increase y a fact r equal t the num er f su - ivisi ns. Theref re, f r this technique t e effective, the w rst case elay etween stages will e ecrease y a fact r f m where m is the num er f a e su - ivisi ns. H wever, if the at mic functi n f the artially i eline architecture has a small stage e-lay, su - ivi ing the stage will achieve n significant ecrease in the w rst case stage elay. In this case, su - i elining w ul result in n significant increase in the system's cl ck frequency ut w ul increase the l gic res urces an cl ck cycles require t erf rm an encry ti n, resulting in re uce thr ugh ut.

Many FPGAs r vi e em e e RAM which may e use t re lace the r un key an -B x multi-lexing har ware. By st ring the keys within the RAM l cks, the a r riate key may e a resse ase n the current r un . H wever, ue t the limite num er f RAM l cks, as well as their restricte it wi th, this meth l gy is n t feasi le f r architectures with many i eline stages r unr lle l s. Th se architectures require m re RAM l cks than are ty ically availa le. A iti nally, the switching time f r the RAM is m re than a fact r f three l nger than that f a stan ar CLB slice element, resulting in the RAM element having a lesser s ee -u effect n the verall im lementati n. Theref re, the use f em e e RAM is n t c nsi ere f r this stu y t maintain c nsistency etween architectural im lementati ns.

5 Architectur l Im lement ti n An lysis

F r each f the AE finalists, the f ur architecture ti ns escri e in ecti n 4.2 were im lemente in VHDL using a tt m-u esign an test meth l gy. The same har ware interface was use f r each f the im lementati ns. R un keys are st re in internal registers an all keys must e l a e ef re encry ti n may egin. Key l a ing is isa le until encry ti n is c m lete . These im lementati ns yiel e a great eal f kn wle ge in regar s t the FPGA suita ility f each AE finalist. What f ll ws is a iscussi n f the kn wle ge gaine regar ing each alg rithm when im lemente using the f ur architecture ty es.

5.1 Architectur l Im lement ti n An lysis — RC6

When im lementing the RC6 alg rithm, it was first etermine that the RC6 m ul 2^{32} multi licati n was the minant element f the r un functi n in terms f require l gic res urces. Each RC6 r un requires tw c ies f the m ul 2^{32} multi lier. H wever, it was f un that the RC6 r un functi n es n t require a general m ul 2^{32} multi lier. The RC6 multi liers im lement the functi n $A(2A +)$ which may e im lemente as $2A^2 + A$. Theref re, the multi licati n erati n was re lace with an array squarer with summe artial r ucts, requiring fewer har ware res urces an resulting in a faster im lementati n. The remaining c m nents f the RC6 r un functi n — fixe an varia le shifting, it-wise X R, an m ul 2^{32} a iti n — were f un t e sim le in structure, resulting in these elements f the r un functi n requiring few har ware res urces. While varia le shifting erati ns have the tential t require c nsi era le har ware res urces, the - it varia le shifting require y the RC6 r un functi n require few har ware res urces. Instea f im lementing a 32-t -1 multi lex r f r each f the thirty-tw r tati n ut ut its (c ntr lle y the five shifting its), a five-level multi lexing a r ach was use . The varia le r tati n is r ken int five stages, each f which is c ntr lle y ne f the five shifting its. F r each r tati n ut ut it f a given stage, a 2-t -1 multi lex r c ntr lle y the stage's shifting it is use . This im lementati n requires a t tal f 160 2-t -1 multi lex rs as se t the thirty-tw 32-t -1 multi lex rs require f r a ne-stage im lementati n. H wever, using 2-t -1 multi lex rs t f rm the five-stage arrel-shifter results in an verall im lementati n that is smaller an faster when c m are t the ne-stage arrel-shifter im lementati n as escri e in [18, ecti n 3.4]. Finally, it was f un that the synthesis t ls c ul n t minimize the verall size f a RC6 r un sufficiently t all w f r a fully unr lle r fully i eline im lementati n f the entire twenty r un s f the alg rithm within the target FPGA.

As iscusse in ecti n 4.2, im lementing a single r un f the RC6 alg rithm r vi es the greatest area- timize s luti n. Further l unr lling r vi e nly min r thr ugh ut increases as the ecrease in

the num er f cycles er encry te l ck was ffset y the ra i ly ecreasing system cl ck frequency. 2-stage artial i elining was f un t yiel the highest thr ugh ut when erating in FB m e, ut erf rming the single r un iterative l ing im lementati n y achieving a significantly higher system cl ck frequency.

When erating in NFB m e, a artially i eline architecture with tw a iti nal su - i eline stages was f un t ffer the a vantage f extremely high thr ugh ut rates nce the latency f the i eline was met, with the 10-stage artial i eline im lementati n is laying the est thr ugh ut an results. Base n the elay analysis f the artial i eline im lementati ns, it was etermine that nearly tw thir s f the r un functi n's ass ciate elay was attri ute t the m ul 2^{32} multi lier. Theref re, tw a iti nal i eline su -stages were im lemente s as t su ivi e the multi lier int smaller l cks, resulting in a t tal f three i eline stages er r un functi n. As a result, an increase y a fact r f m re than 2. was seen in the system's cl ck frequency, resulting in a similar increase in thr ugh ut when erating in NFB m e. Further su - i elining was n t im lemente as this w ul require su - ivi ing the a ers use t sum the artial r ucts (a n n-trivial task) t alance the elay etween su - i eline stages.

5.2 Architectur l Im lement ti n An lysis — Rijn el

When im lementing the Rijn ael alg rithm, it was first etermine that the Rijn ael -B xes were the minant element f the r un functi n in terms f require l gic res urces. Each Rijn ael r un requires sixteen c ies f the -B xes, each f which is an 8- it t 8- it l k-u -ta le, requiring significant har ware res urces. H wever, the remaining c m nents f the Rijn ael r un functi n — yte swa ing, c nstant Gal is fiel multi licati n, an key a iti n — were f un t e sim le in structure, resulting in these elements f the r un functi n requiring few har ware res urces. A iti nally, it was f un that the synthesis t ls c ul n t minimize the verall size f a Rijn ael r un sufficiently t all w f r a fully unr lle r fully i eline im lementati n f the entire ten r un s f the alg rithm within the target FPGA.

ur risingly, a ne r un artially i eline im lementati n with ne su - i eline stage r vi e the m st area- timize s luti n. As c m are t a ne-stage im lementati n with n su - i elining, the a iti n f a su - i eline stage aff r e the synthesis t l greater flexi ility in its timizati ns, resulting in a m re area efficient im lementati n. While 2-stage l unr lling was f un t yiel the highest thr ugh ut when erating in FB m e, the measure thr ugh ut was within 10% f the single stage im lementati n. Due t the r a ilistic nature f the lace-an -r ute alg rithms, ne can ex ect a variance in erf rmance ase n ifferences in the starting int f the r cess. When erf rming this r cess multi le times, kn wn as multi- ass lace-an -r ute, it is likely that the single r un im lementati n w ul achieve a thr ugh ut similar t that f the 2-stage l unr lle im lementati n.

When erating in NFB m e, artial i elining was f un t ffer the a vantage f extremely high thr ugh ut rates nce the i eline latency was met, with the -stage artial i eline im lementati n is laying the est thr ugh ut results. While Rijn ael cann t e im lemente using a fully i eline architecture ue t the large size f the r un functi n, significant thr ugh ut increases were seen as c m are t the l unr lling architecture.

u - i elining f the artially i eline architectures was im lemente y inserting a i eline su -stage within the Rijn ael r un functi n. Base n the elay analysis f the artial i eline im lementati ns, it was etermine that nearly half f the r un functi n's ass ciate elay was attri ute t the -B x su stituti ns. Theref re, the a iti nal i eline su -stage was im lemente s as t se arate the -B xes fr m the rest f the r un functi n. As a result, an increase y a fact r f nearly 2 was seen in the system's cl ck frequency, resulting in a similar increase in thr ugh ut when erating in NFB m e. Further su - i elining was n t im lemente as this w ul require su - ivi ing the -B xes (a n n-trivial task) t alance the elay etween su - i eline stages.

5.3 Architectur l Im lement ti n An lysis — Ser ent

When im lementing the er ent alg rithm, it was first etermine that since the er ent -B xes are relatively small (4- it t 4- it), it is ssi le t im lement them using c m inati nal l gic as se t mem ry elements. A iti nally, the -B xes ma extremely well t the Xilinx CLB slice, which is c m rise f 4- it l k-u -ta les, all wing ne -B x t e im lemente in a t tal f tw CLB slices, yiel ing a c m act im lementati n which minimizes r uting etween CLB slices. Finally, the c m nents f the er ent r un functi n — key masking, -B x su stituti n, an linear transf rmati n — were f un t e sim le in structure, resulting in the r un functi n requiring few har ware res urces.

Im lementing a single r un f the er ent alg rithm r vi es the greatest area- timize s luti n. H wever, a significant erf rmance im r vement was achieve y erf rming 8-r un l unr lling, rem v- ing the nee f r -B x multi lexing har ware as ne c y f each ssi le -B x gr u ing is n w inclu e within ne f the eight r un s. This am unt f l unr lling achieve a significant erf rmance increase with little increase in har ware res urces ue t the c m act nature f the er ent r un functi n. As ex- ecte , unr lling thirty-tw r un s f the er ent alg rithm resulte in a lesser erf rmance when c m are t the eight r un im lementati n. Im lementing the thirty-tw r un s f the alg rithm in c m inat rial l gic severely ham ere the verall cl ck frequency f the system, verri ing the erf rmance increase cause y the rem val f the multi lexing har ware require t switch etween keys.

When erating in NFB m e, a full-length i eline architecture was f un t ffer the a vantage f extremely high thr ugh ut rates nce the latency f the i eline was met, ut erf rming smaller artially i eline im lementati ns. In the fully i eline architecture, all f the elements f a given r un functi n are im lemente as c m inat rial l gic. ther AE finalists cann t e im lemente using a fully i eline architecture ue t the larger r un functi ns. H wever, ue t the small size f the er ent -B xes (4- it l k-u -ta les), the c st f -B x re licati n is minimal in terms f the require har ware.

Finally, su - i elining f the artially i eline architectures was etermine t yiel n thr ugh ut increase. Because the r un functi n c m nents are all sim le in structure, there is little erf rmance t e gaine y su ivi ing them with registers in an attem t t re uce the elay etween stages. As a result, the increase in the system's cl ck frequency w ul n t utweigh the increase in the num er f cl ck cycles require t erf rm an encry ti n, resulting in a erf rmance egra ati n.

5.4 Architectur l Im lement ti n An lysis — Tw fish

When im lementing the Tw fish alg rithm, it was first etermine that the synthesis t ls were una le t minimize the Tw fish -B xes t the extent f ther AE finalist alg rithms ue t the -B xes eing key- e en ent. Theref re, the verall size f a Tw fish r un was t large t all w f r a fully unr lle r fully i eline im lementati n f the alg rithm within the target FPGA. M re ver, the key- e en ent -B xes were f un t require nearly half f the elay ass ciate with the Tw fish r un functi n.

As ex ecte , im lementing a single r un f the Tw fish alg rithm r vi es the greatest area- timize s luti n in terms f t tal CLB slices require f r the im lementati n. A iti nal l unr lling r vi e min r thr ugh ut increases as the ecrease in the num er f cycles er encry te l ck was ffset y the ra i ly ecreasing system cl ck frequency. H wever, single stage artial i elining with ne su - i eline stage was f un t yiel the est thr ugh ut an when erating in fee ack m e. With a small increases in the require har ware res urces, the su - i eline architecture was a le t reach a significantly faster system cl ck frequency as c m are t the l unr lling an artial i eline im lementati ns.

When erating in NFB m e, a artially i eline architecture was f un t ffer the a vantage f extremely high thr ugh ut rates nce the latency f the i eline was met, with the 8-stage artial i eline im lementati n is laying the est thr ugh ut results. While Tw fish cann t e im lemente using a fully i eline architecture ue t the large size f the r un functi n, significant thr ugh ut increases were seen as c m are t the l unr lling architecture.

Finally, su - i elining f the artially i eline architectures was im lemente y inserting a i eline su -stage within the Tw fish r un functi n. Base n the elay analysis f the artial i eline im lementati ns, it was etermine that nearly half f the r un functi n's ass ciate elay was attri ute t the -B x su stituti ns. Theref re, the a iti nal i eline su -stage was im lemente s as t se arate the -B xes fr m the rest f the r un functi n. As a result, an increase y a fact r f nearly 2 was seen in the system's cl ck frequency, resulting in a similar increase in thr ugh ut when erating in NFB m e. Further su - i elining was n t im lemente as this w ul require su - ivi ing the -B xes (a n n-trivial task) t alance the elay etween su - i eline stages.

6 Perf rm nce Ev lu ti n

Ta les 2 an 3 etail the thr ugh ut measurements f r the im lementati ns f the three architecture ty es f r each f the AE finalists f r th NFB an FB m e. The architecture ty es — l unr lling (LU), full r artial i elining (PP), an artial i elining with su - i elining (P) — are liste al ng with the num er f stages an (if necessary) su - i eline stages in the ass ciate im lementati n; e.g., LU-4 im lies a l unr lling architecture with f ur r un s, while P-2-1 im lies a artially i eline architecture with tw stages an ne su - i eline stage er i eline stage. As a result, the P-2-1 architecture im lements tw r un s f the given ci her with a t tal f tw stages er r un . Thr ugh ut is calculate as:

$$Throughput := (128\ Bits * Cl\ ck\ Frequency)/(Cycles\ Per\ Encry\ te\ Bl\ ck)$$

N te that the im lementati n f a ne stage artial i eline architecture, an iterative l ing architecture, an a ne r un l unr lle architecture are all equivalent an are theref re n t liste se arately. Als n te that the c m ute thr ugh ut f r im lementati ns that em l y any f rm f har ware i elining (as iscusse in ecti n 4) are ma e assuming that the i eline latency has een met.

The num er f CLBs require as well as the maximum erating frequency f r each im lementati n was taine fr m the Xilinx re rt files. N te that the Xilinx t ls assume the a s lute w rst ssi le erating c n iti ns — highest ssi le erating tem erature, l west ssi le su ly v ltage, an w rst-case fa ricati n t lerance f r the s ee gra e f the FPGA [23]. As a result, it is c mm n f r actual im lementati ns t achieve slightly etter erf rmance results than th se s ecifie in the Xilinx re rt files.

While this stu y f cuses n high thr ugh ut im lementati ns, the har ware res urces require t achieve this thr ugh ut is als a critical arameter. N esta lishe metric exists t measure the har ware res urce c sts ass ciate with the measure thr ugh ut f an FPGA im lementati n. Tw area measurements f FPGA utilizati n are rea ily a arent — l gic gates an CLB slices. It is im rtant t n te that the l gic gate c unt es n t yiel a true measure f actual FPGA utilizati n. Har ware res urces within CLB slices may n t e fully utilize y the lace-an -r ute s ftware s as t relieve r uting c ngesti n. This results in an increase in the num er f CLB slices with ut a c rres n ing increase in l gic gates. T achieve a m re accurate measure f chi utilizati n, CLB slice c unt was ch sen as the m st relia le area measurement. Theref re, t measure the har ware res urce c st ass ciate with an im lementati n's resultant thr ugh ut, the Thr ugh ut Per lice (TP) metric is use . We efine TP as:

$$TPS := (Encry\ ti\ n\ Rate)/(\#\ CLB\ lices\ Use\ )$$

Theref re, the timal im lementati n will is lay the highest thr ugh ut an have the largest TP . N te that the TP metric ehaves inversely t the classical time-area (TA) r uct.

Alg.	Arch.	Thr ugh ut (G it/s)		Slices	TPS
RC6	P-10-2	**2.40**		108 6	220881
Rijn ael	P- -1	**1. 4**		10 2	1762 7
er ent	PP-32	**4.86**		004	3 778
Tw fish	P-8-1	**1.5**		34	16 63

Ta le 4: AE finalist erf rmance evaluati n — n n-fee ack m e s ee - timize im lementati ns

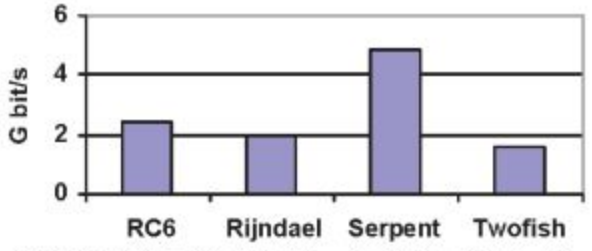

Figure 1: Best thr ugh ut — n n-fee ack m e

Alg.	Arch.	Thr ugh ut (M it/s)		Slices	TPS
RC6	PP-2	**126.5**		318	3 662
Rijn ael	LU-2	**300.1**		302	660
er ent	LU-8	**444.2**		7 64	771
Tw fish	P-1-1	**11 .6**		30 3	3 16

Ta le : AE finalist erf rmance evaluati n — fee ack m e s ee - timize im lementati ns

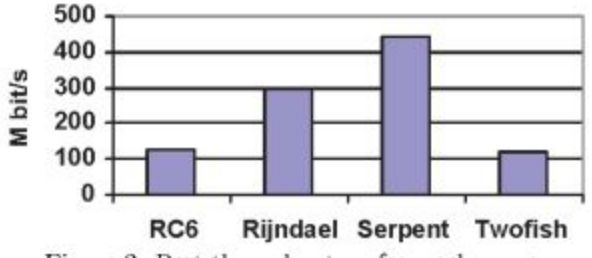

Figure 2: Best thr ugh ut — fee ack m e

Ta les 4 an etail the timal im lementati ns f the AE finalists in th FB an NFB m es. A iti nally, TP is als sh wn f r each f the im lementati ns. It is critical t n te that f r the ur ses f this stu y, the timal im lementati n f r an AE finalist is efine t yiel the highest thr ugh ut. *As pr vi usly discuss d, th synth sis t ls w r s t t ptimiz f r sp d t guarant that th high st thr ughputs w uld b achi v d f r ach impl m ntati n. H w v r, sh uld an ptimal impl m ntati n b d fin d bas d n ith r TP r ar a, th impl m ntati n r sults sh wn in Tabl s 2 and 3 (and, as a r sult, th s sh wn in tabl s 4 and 5 as w ll) ar n l ng r r pr s ntativ f th b st p ssibl impl m ntati ns f r th archit ctur s studi d. T achi v a tru r pr s ntati n that d fin s ptimality bas d n ith r TP r ar a, synth sis must b p rf rm d with th t ls s t t ptimiz f r ar a.* While an area-efficiency analysis f the AE finalists warrants investigati n, it is ey n the sc e f this stu y.

Base n the ata sh wn in Ta les 4 an , the er ent alg rithm clearly ut erf rms the ther AE finalists in th m es f erati n. As c m are t its nearest c m etit r, er ent exhi its a thr ugh ut increase f a fact r 2.2 in NFB m e an a fact r 1. in FB m e. Interestingly, RC6, Rijn ael, an Tw fish

all exhi it similar erf rmance results in NFB m e. H wever, Rijn ael exhi its significantly im r ve erf rmance in FB m e as c m are t RC6 an Tw fish, alth ugh it is still 0% sl wer than er ent.

ne f the main fin ings f ur investigati n, namely that er ent a ears t e es ecially well suite f r an FPGA im lementati n fr m a erf rmance ers ective, seems es ecially interesting c nsi ering that er ent is clearly n t the fastest alg rithm with res ect t m st s ftware c m aris ns [ ]. An ther maj r result f ur stu y is that all f ur alg rithms c nsi ere easily achieve Giga it encry ti n rates with stan ar c mmercially availa le FPGAs. The alg rithms are at least ne r er f magnitu e faster than the est re rte s ftware realizati ns. These s ee -u s are essentially achieve y arallelizati n (i elining an su - i elining) f the l structure an y wi e eran r cessing (e.g., r cessing f 128 its in nce cl ck cycle), th f which are n t feasi le n current r cess rs. We w ul like t stress that the i eline architectures cann t e use t their maximum a ility f r m es f erati n which require fee ack (CFB, FB, etc.) H wever we elieve that f r many a licati ns which require high encry ti n rates, n n-fee ack m es (r m ifie fee ack m es such as interleave CFB [3, ecti n .12]) will e the m es f ch ice. N te that the C unter M e grew ut f the nee f r high s ee encry ti n f ATM netw rks which require arallelizati n f the encry ti n alg rithm.

7 C nclusi ns

The im rtance f the A vance Encry ti n tan ar an the significance f high thr ugh ut im lementati ns f the AE finalists has een examine . A esign meth l gy was esta lishe which in turn le t the architectural requirements f r a target FPGA. The c re erati ns f the AE finalists were i entifie an multi le architecture ti ns were iscusse . The im lementati n f each architecture ti n f r each f the AE finalists was analyze t etermine their suita ility f r har ware im lementati n. Base n the im lementati n results, the est s ee - timize im lementati ns were i entifie f r each AE finalist in th n n-fee ack an fee ack m es. U n c m aris n, it was etermine that the er ent alg rithm yiel e the est erf rmance in th m es, where est erf rmance was efine strictly as the highest thr ugh ut. The er ent alg rithm ut erf rms its nearest c m etit r y a fact r f 2.2 in n n-fee ack m e an y a fact r f 1. in fee ack m e.

8 Ackn wle gement

We w ul like t thank Pawel Ch wiec an Kris Gaj fr m Ge rge Mas n University f r their hel ful iscussi n an the VHDL c e m ules that were r vi e t assist in the im lementati n f s me f the AE finalists. We w ul als like t thank Alan Martell fr m the University f Pitts urgh f r his u lic- main VHDL c e m ule that was use in im lementati n f the AE finalists.

References

[1] D. tins n, *rypt graphy, Th ry and Practic* . B ca Rat n, FL: CRC Press, 1 .

[2] Nati nal Institute f tan ar s an Techn l gy (NI T), *c nd Advanc d Encrypti n tandard (AE) nf r nc* , (R me, Italy), March 1 .

[3] B. chneier, *Appli d rypt graphy*. J hn Wiley & ns Inc., 2n e ., 1 .

[4] R. D u , "Har ware Cry t luti ns B st VPN," *EETim s*, . 7–64, A ril 1 .

[ ] B. Gla man, "Im lementati n Ex erience with AE Can i ate Alg rithms," in *Pr c dings: c nd AE andidat nf r nc (AE 2)*, (R me, Italy), March 1 .