Hardware optimierte leichtgewichtige Blockchiffren für RFID- und Sensor-Systeme

Christof Paar und Axel Poschmann
Horst Görtz Institut für IT Sicherheit
Lehrstuhl für Kommunikationssicherheit
Ruhr-Universität Bochum
{cpaar,poschmann}@crypto.rub.de

Abstract: In diesem Artikel wird ein Überblick über leichtgewichtige Kryptographie (lightweight Cryptography) gegeben. Weiterhin werden die beiden neuen auf Hardware optimierten Chiffren DESL und PRESENT näher vorgestellt. Der anschließende Vergleich der Implementierungsergebnisse mit anderen kürzlich vorgeschlagenen Blockchiffren wie mCrypton, HIGHT oder CLEFIA zeigt, dass DESL und PRESENT weniger Chipfläche verbrauchen. Ebenfalls können beide Algorithmen überraschenderweise sogar mit kürzlich veröffentlichten, auf Hardware optimierten Stromchiffren (Trivium und Grain) konkurrieren.

Keywords: RFID, DESL, PRESENT, lightweight cryptography

1 Motivation

Die Schlagwörter *Ubiquitous* und *Pervasive Computing* bezeichnen die vollständige Durchdringung unseres Alltags mit intelligenten Geräten. *Kabellose Sensor-Netzwerke* (Wireless Sensor Network, *WSN*) und *RFID* (Radio Frequency IDentification, Funkerkennung) sind hierfür zwei Beispiele, die bereits heute vermehrt zum Einsatz kommen. Durch Einsatz der *RFID*-Technologie lassen sich beispielsweise in der Logistik große Einsparpotenziale ausnutzen. Auf der anderen Seite birgt die vollständige Durchdringung von intelligenten Geräten auch große Gefahren für die Privatsphäre bzw. Anonymität, weil die gesammelten Daten für das Anlegen von Bewegungsprofilen o.ä. mißbraucht werden könnten. Eine geeignete Gegenmaßnahme stellt die Leser-seitige Authentifizierung dar: Wenn sich jedes Lesegerät bei dem zu lesenden *RFID*-Tag authentifizieren müsste, könnte das unbefugte Ausspähen von Daten unterbunden werden. Dies kann mit Hilfe eines *Challenge and Response* Protokolls realisiert werden, das unter anderem auf eine symmetrische Chiffre zurückgreift.

Für *Ubiquitous* bzw. *Pervasive Computing* werden kostengünstige Geräte benötigt, die kabellos miteinander kommunizieren können. Viele dieser Geräte verfügen über keine eigene Stromversorgung (passive Geräte) sondern beziehen ihre Energie aus dem elektromagnetischen Feld (Funkwelle), über das sie auch kommunizieren. Aktive Geräte hingegen beinhalten eine Batterie, die sie mit Energie versorgt. Idealerweise sollten diese Batterien

mehrere Monate bis Jahre ausreichen um das Gerät mit Energie zu versorgen. Sowohl für aktive als auch für passive Geräte ist ein geringer Stromverbrauch also eine Grundanforderung.

Weiterhin sind die zum Einsatz kommenden Geräte bereits aus Kostengründen stark in ihrer Rechenleistung und des zur Verfügung stehenden Speichers beschränkt. Daher bietet es sich für kryptographische Operationen an, einen Co-Prozessor zu implementieren, beispielsweise in Form eines *ASICs* (Application Specific Integrated Circuit, anwendungsspezifischer integrierter Schaltkreis). Denn im Vergleich zu *FPGA*- (Field Programmable Gate Array) oder Software-Implementierungen gewährleisten *ASICs* eine kompakte und effiziente Implementierung bei begrenzter Leistungsaufnahme. Der Fertigungspreis pro ASIC ist ungefähr proportional zur verbrauchten Siliziumfläche, wenn man die einmaligen Kosten für die lithographische Maske und den Entwurf vernachlässigt.

Moore's Gesetz muss hier anders als bisher interpretiert werden, denn statt der Verdoppelung der Rechenleistung bzw. der Speicherkapazität reduzieren sich die Kosten für gleichbleibende Rechenleistung, Speicherkapazität oder Siliziumfläche alle 18 Monate um die Hälfte. Als Folge ist zu erwarten, dass die Anzahl der Anwendungen für *WSNs* oder *RFID* kontinuierlich steigt (und damit die Anzahl der eingesetzen Geräte), während die Geräte weiterhin beschränkt in ihren Ressourcen bleiben. Daraus ergibt sich ein konstant hoher Bedarf für leichtgewichtige Kryptographie. Aus den oben genannten Gründen wurden in letzter Zeit vermehrt auf Hardware optimierte Chiffren vorgeschlagen [HSH+06, SSA+07, LK]. Dabei muss beachtet werden, dass das Hauptentwurfsziel bei den Chiffren HIGHT und CLEFIA ein gutes Flächen-Zeit-Produkt war und weniger ein minimaler Flächenverbrauch. Im Gegensatz hierzu haben wir uns bei dem Entwurf von DESL und PRESENT bewusst auf Effizienzeigenschaften einer kostengünstigen *ASIC* Implementierung beschränkt, weil wir Hardware-Implementierungen für *RFID* und andere ressourcenbeschränkte Geräte als Haupteinsatzgebiet für DESL und PRESENT sehen. Das wichtigste Entwurfsziel war es, den Flächenverbrauch zu minimieren. An zweiter Stelle stand die Optimierung des Stromverbrauchs.

2 Die Blockchiffre DESL

Als Ausgangspunkt wurde der *Data Encryption Standard* (DES [MvOV97]) Algorithmus gewählt, weil dieser speziell auf Hardware optimiert wurde, während der Rijndael Algorithmus (Advanced Encryption Standard, AES) unter anderem für seine gute Software-Effizienz bekannt ist. Zusätzlich ist DES in den 30 Jahren seit seiner Veröffentlichung besser untersucht worden als jede andere Chiffre. Es wurden insgesamt nur drei Attacken gefunden, die besser sind als eine vollständige Schlüsselsuche: Die Lineare und die Differentielle Kryptanalyse [Mat94, BS92] und die Davies-Murphy-Attacke [DM95].

Die Vielzahl der DES-Varianten, die vor der Entdeckung der Differentiellen und der Linearen Kryptanalyse vorgeschlagen wurden (z.B. GDES), konnten im Gegensatz zu unserer Variante DESL nicht auf den Erkenntnissen dieser starken Attacken aufbauen. Daher glauben wir, dass eine Chiffre, die eine minimale und genau begründete Veränderung an einer

sehr gut untersuchten Chiffre vornimmt, vertraulicher ist als eine komplett neu entwickelte.

Die *Initiale Permutation* (IP) am Anfang und die *Inverse Initiale Permuation* (IP^{-1}) am Ende von DES bieten keinerlei kryptographischen Zusatznutzen, daher haben wir sie bei DESL weggelassen. Der einzige weitere Unterschied zwischen DES und DESL besteht in der nicht-linearen Substitutions-Ebene. Wir haben die acht originalen S-Boxen von DES gegen *eine* neue, achtfach wiederholte S-Box ausgetauscht. Bei der Auswahl der neuen S-Box haben wir besondere Sorgfalt walten lassen. Es wurden sowohl die originalen S-Box Entwurfskriterien berücksichtigt, die erstmal 1994 von Don Coppersmith, einem der ursprünglichen Entwickler des DES, veröffentlicht wurden [Cop94], als auch neue Kriterien definiert. Diese neuen Kriterien erschweren besonders die drei bekannten Angriffe auf DES. Als Ergebnis unserer neuen Entwurfskriterien haben wir eine S-Box gewählt, die kryptographisch besonders robust ist. Eingebettet in die DES-Struktur erhält man mit Hilfe dieser neuen S-Box einen Algorithmus, der gegen die oben genannten Attacken resistent ist. Das bedeutet, die Lineare und die Differentielle Kryptanalyse und die Davies-Murphy-Attacke auf unseren DESL sind entweder unmöglich oder erfordern einen größeren Aufwand als eine vollständige Schlüsselsuche.

DES wurde häufig aufgrund seiner zu kurzen Schlüssellänge kritisiert. Für viele Anwendungen sollten 56-Bit Schlüssel dennoch ausreichend sein. Wenn darüber hinaus ein höheres Sicherheitsniveau erwünscht ist, bietet unser DESL die Möglichkeit auf einfache Weise den Schlüsselraum zu vergrößern. Genau wie DESX [KR96] nutzt unsere Erweiterung von DESL, DESXL, sogenanntes *Prewhitening* und *Postwhitening* um den Schlüsselraum auf 184-Bits zu erhöhen. Dabei werden sowohl der Klartext vor der Verschlüsselung mit einem 64-Bit Schlüssel XOR addiert (prewhitening) als auch der resultierende Geheimtext mit einem zweiten 64-Bit Schlüssel (postwhitening) XOR addiert. Für eine detaillierte Sicherheitsanalyse und weitere Details verweisen wir den interessierten Leser auf [LPPS07].

3 Die Blockchiffre PRESENT

Im Anschluss an die Entwicklung von DESL und DESXL war geplant den AES dahingehend zu verändern, dass der Flächenverbrauch minimiert wird. Die Wahl fiel zuerst auf den AES-Finalisten Serpent, der die besten Hardware-Resultate bot. Es zeigte sich jedoch bald, dass es einfacher ist, einen komplett neuen Algorithmus zu entwerfen als den Flächenverbrauch von Serpent zu minimieren. Dennoch trägt der Name PRESENT der Ausgangsüberlegung immer noch Rechnung.

PRESENT ist ein Substitutions-Permutations-Netzwerk mit 32 Runden, 64-Bit Blocklänge und 80- bzw. 128-Bit Schlüssellänge[1]. Eine Runde setzt sich aus drei Schritten zusammen: 1. KeyAdd, 2. Substitutions-Layer und 3. Permutations-Layer. Im ersten Schritt wird der Rundenschlüssel mit dem Datenwort XOR-addiert (KeyAdd). Der Substitutions-Layer besteht aus 16 identischen S-Boxen mit je vier Eingangs- und je vier Ausgangs-

[1] Im folgenden werden wir uns auf die 80-Bit Variante PRESENT-80 konzentrieren, weil wir glauben, dass diese Schlüssellänge ausreichend für die zu erwartenden Anwendungsgebiete ist.

Bits (4x4 S-Box). Der Permutations-Layer wird durch eine Bit-Permutation realisiert. Der Schlüsselerzeugungs-Algorithmus besteht aus einer 61-Bit Links-Rotation, einer S-Box und einer XOR-Addition mit einem Rundenzähler. Die Grundphilosophie bei dem Entwurf von PRESENT war Einfachheit. So haben wir uns bewusst für nur eine S-Box ebtschieden, die sowohl mehrfach im Datenpfad als auch bei der Schlüsselerzeugung zum Einsatz kommt. Desweiteren wurde eine S-Box mit vier Eingangs- und vier Ausgangsbits gewählt, weil dies den Flächenbedarf im Vergleich zu 8x8 S-Boxen erheblich (25 GE vs. 120 GE) verringert. Bit-Permutationen sind im Gegensatz zu Software-Implementierungen in Hardware sehr effizient, weil keine Transistoren benötigt werden. Die Realisierung erfolgt alleine über Verkabelung, wodurch sowohl der Flächen- als auch der Stromverbrauch verringert wird. Für eine detaillierte Sicherheitsanalyse [2] von PRESENT sowie weitere Details verweisen wir den interessierten Leser auf [BKL+07].

4 Implementierungsergebnisse

	Key Bits	Block Bits	Takte pro Block	Durchsatz bei 100KHz (Kbps)	Logic Process	Fläche GE
Blockchiffren						
PRESENT-80 [BKL+07]	80	64	32	200	0.18μm	1570
AES-128 [FWR05]	128	128	1032	12.4	0.35μm	3400
HIGHT [HSH+06]	128	64	1	6400	0.25μm	3048
CLEFIA [SSA+07]	128	128	36	355.56	0.09μm	4993
mCrypton [LK]	96	64	13	492.3	0.13μm	2681
DES [LPPS07]	56	64	144	44.4	0.18μm	2309
DESXL [LPPS07]	184	64	144	44.4	0.18μm	2168
Stromchiffren						
Trivium [GB07]	80	1	1	100	0.13μm	2599
Grain [GB07]	80	1	1	100	0.13μm	1294

Die acht identischen S-Boxen des DESL erlauben es, eine Runde von DESL effizient zu serialisieren. Dadurch können im Vergleich zu einer serialisierten Implementierung von DES 20% der Transistoren eingespart werden. PRESENT-80 ist bei einer größeren Schlüssellänge dennoch kleiner in Hardware als DESL und hat zusätzlich einen größeren Durchsatz. Vergleicht man diese Zahlen mit den aktuellen eSTREAM Kandidaten [GB07] fällt auf, dass PRESENT vom Flächenverbrauch her der zweitkleinste Algorithmus ist. Dies ist um so erstaunlicher, als dass gemeinhin angenommen wird, dass Stromchiffren genau in diesem Vergleichskriterium Blockchiffren überlegen sind.

Da sowohl DESL als auch PRESENT neue Entwürfe sind, die sich erst noch als sicher erweisen müssen, möchten wir zu einer Analyse beider Algorithmen ermutigen.

[2] U.a. werden Lineare, Differentielle, Strukturelle, Algebraische und Schlüsselerzeugungs-Attacken untersucht.

Literatur

[BKL+07] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin und C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In *submitted to CHES 2007*, 2007.

[BS92] E. Biham und A. Shamir. Differential Cryptanalysis of the Full 16-Round DES. In *CRYPTO '92*, Seiten 487–496, 1992. available for download at `citeseer.ist.psu.edu/biham93differential.html`.

[Cop94] D. Coppersmith. The Data Encryption Standard (DES) and its Strength Against Attacks. Technical report rc 186131994, IBM Thomas J. Watson Research Center, December 1994.

[DM95] D. Davies und S. Murphy. Pairs and Triplets of DES S-Boxes. *Journal of Cryptology*, 8(1):1–25, 1995.

[FWR05] M. Feldhofer, J. Wolkerstorfer und V. Rijmen. AES Implementation on a Grain of Sand. *Information Security, IEE Proceedings*, 152(1):13–20, 2005.

[GB07] T. Good und M. Benaissa. Hardware Results for selected Stream Cipher Candidates. State of the Art of Stream Ciphers 2007 (SASC 2007), Workshop Record, February 2007.

[HSH+06] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim und S. Chee. HIGHT: A New Block Cipher Suitable for Low-Resource Device . In L. Goubin und M. Matsui, Hrsg., *Proceedings of CHES 2006*, number 4249 in LNCS, Seiten 46–59. Springer Verlag, 2006.

[KR96] J. Kilian und P. Rogaway. How to Protect DES against Exhaustive Key Search. In N. Koblitz, Hrsg., *Advances in Cryptology — CRYPTO '96*, Jgg. Lecture Notes in Computer Science, Seiten 252–267, Berlin, Germany, 1996. Springer-Verlag.

[LK] C. Lim und T. Korkishko. mCrypton - A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors. In *Proceedings of the Workshop on Information Security Applications - WISA'05*, LNCS.

[LPPS07] G. Leander, C. Paar, A. Poschmann und K. Schramm. New Lighweight DES Variants. In *Proceedings of FSE 2007*. LNCS, Springer-Verlag, to appear, 2007.

[Mat94] M. Matsui. Linear Cryptanalysis of DES Cipher. In T. Helleseth, Hrsg., *Advances in Cryptology — EUROCRYPT '93*, Jgg. LNCS 0765, Seiten 286 – 397, Berlin, Germany, 1994. Springer-Verlag.

[MvOV97] A. J. Menezes, P. C. van Oorschot und S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, Florida, USA, first. Auflage, 1997.

[SSA+07] T. Shirai, K. J. Shibutani, T. Akishita, S. Moriai und T. Iwata. The 128-Bit Blockcipher CLEFIA. In *Proceedings of FSE 2007*. LNCS, Springer-Verlag, to appear, 2007.