Simon: NSA-designed Cipher in the Post-snowden World

Tomer Ashur

KU Leuven

28/12/2015

The SIMON and SPECK Families of Lightweight Block Ciphers

- Two families of lightweight block ciphers (10 variants for each)

The SIMON and SPECK Families of Lightweight Block Ciphers

- Two families of lightweight block ciphers (10 variants for each)
- Desgined by the NSA

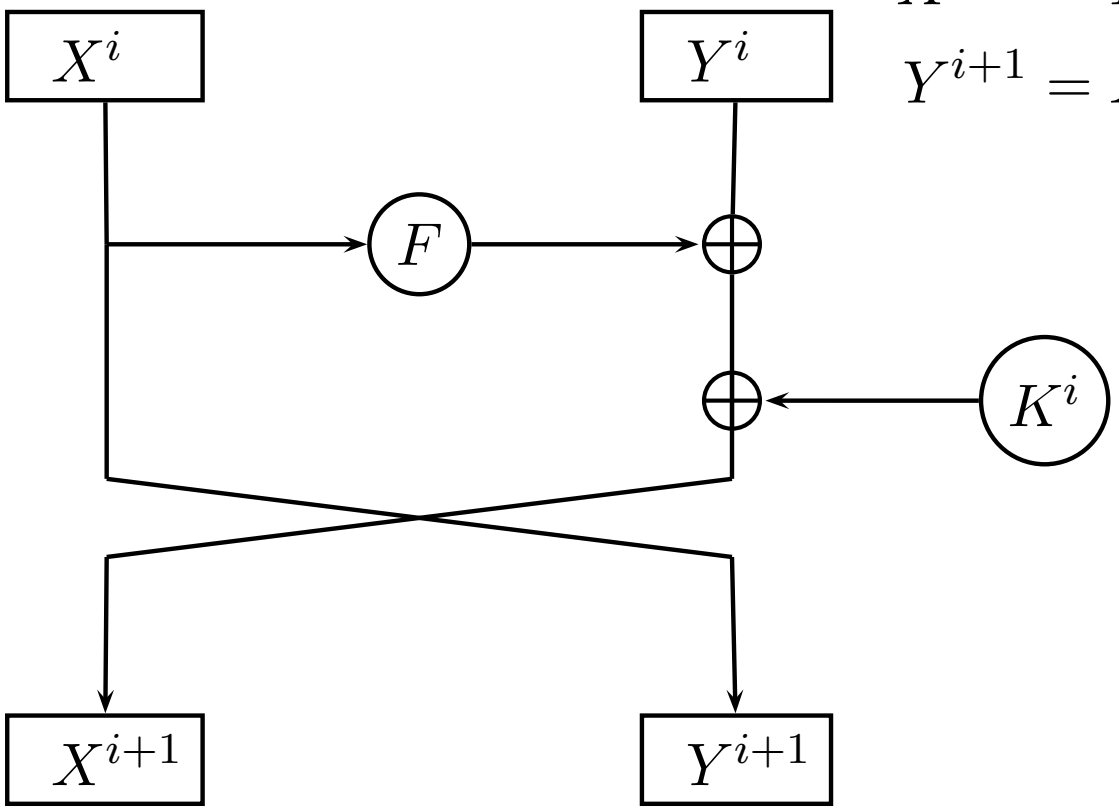
The SIMON and SPECK Families of Lightweight Block Ciphers

- Two families of lightweight block ciphers (10 variants for each)
- Desgined by the NSA
- Released in 2013

- Hardware oriented

- Hardware oriented
- Fesitel structure

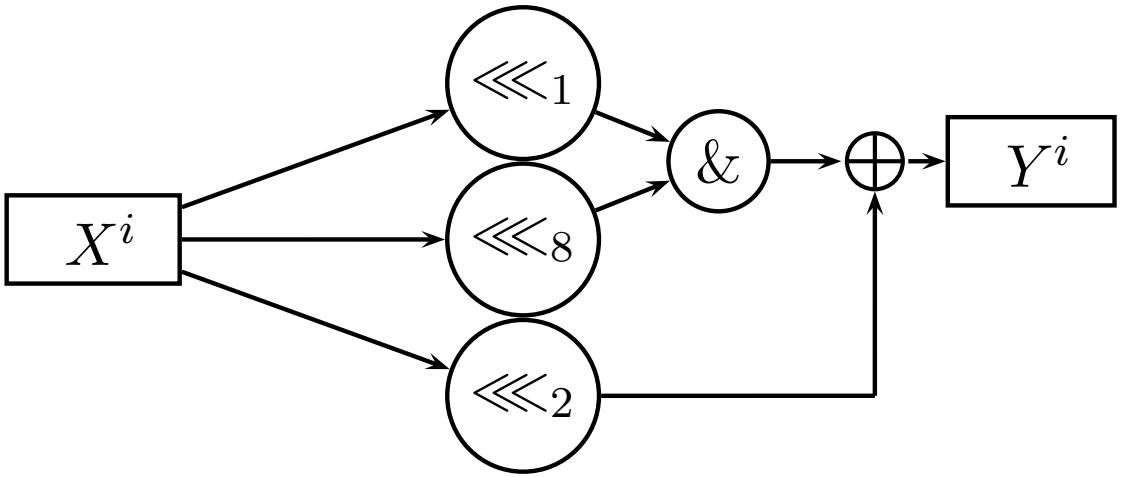
Simon - Structure



$$X^{i+1} = F(X^i) \oplus Y^i \oplus K^i$$
$$Y^{i+1} = X^i$$

Block size	Key size	No. rounds
32	64	32
48	72	36
	96	36
64	96	42
	128	44
96	96	52
	144	54
128	128	68
	192	69
	256	72

Simon - Round Function



Simon - Key schedule

Simon - Performance

		hardware		software		
size	name	area (GE)	throughput (kbps)	flash (bytes)	SRAM (bytes)	throughput (kbps)
48/96	SIMON	763	15.0	196	0	589
	SPECK	884	12.0	134	0	943
	EPCBC	1008	12.1	[365]	0	[93]
64/80	TWINE	1011	16.2	1304	414	472
	PRESENT	1030	12.4	[487]	0	96
	PICCOLO	1043	14.8	–	–	–
	KATAN	1054	25.1	272	18	14
	KLEIN	1478	23.6	766	18	168
64/96	SIMON	838	17.8	274	0	540
	SPECK	984	14.5	182	0	888
	KLEIN	1528	19.1	[766]	[18]	[134]
64/128	SIMON	1000	16.7	282	0	515
	SPECK	1127	13.8	186	0	855
	PICCOLO	1334	12.1	–	–	–
	PRESENT	1339	12.1	[487]	[0]	[96]

Figure: Performance figures from the original paper (eprint 2013/404)

Simon - Performance

size	algorithm	area (GE)	tput (kbps)	ref
48/96	Simon	739	5.0	[9]
	Speck	794	4.0	[9]
64/80	TWINE	1011	16.2	[57]
	PRESENT	1030	12.4	[65]
	Piccolo	1043	14.8	[52]
	Katan	1054	25.1	[22]
	KLEIN	1478	23.6	[33]
64/96	Simon	809	4.4	[9]
	Speck	860	3.6	[9]
	KLEIN	1528	19.1	[33]
64/128	Simon	958	4.2	[9]
	Speck	996	3.6	[9]
	Piccolo	1334	12.1	[52]
	PRESENT	1339	12.1	[65]
96/96	Simon	955	3.7	[9]
	Speck	1012	3.4	[9]
128/128	Simon	1234	2.9	[9]
	Speck	1280	3.0	[9]
	AES	2400	56.6	[41]

Figure: Performance figures from the NIST workshop (eprint 2015/585)

Simon - Security

- " ...SIMON and SPECK have been designed to provide security against traditional adversaries who can adaptively encrypt and decrypt large amounts of data. We concede that (as is the case with other algorithms) there will be what amount to highly optimized ways to exhaust the key that reduce the cost of a naive exhaust by a small factor. We have also made a reasonable effort to provide security against adversaries who can flip key bits, and our aim is that there should be no related-key attacks... " (eprint 2013/404)

- "The development process culminated in the publication of the algorithm specifics in June 2013 [9]. Prior to this, Simon and Speck were analyzed by NSA cryptanalysts and found to have security commensurate with their key lengths; i.e., no weaknesses were found. Perhaps more importantly, the algorithms have been pretty heavily scrutinized by the international cryptographic community for the last two years (see, e.g., [2], [3], [5], [4], [1], [6], [15], [16], [20], [27], [29], [37], [47], [51], [53], [56], [59], [62], [60], [30], [7], [25], [42], [24])." (eprint 2015/585)

$$X_i \& Y_i = \begin{cases} 0 & p = \frac{3}{4}; \epsilon = \frac{1}{4} \\ X_i & p = \frac{3}{4}; \epsilon = \frac{1}{4} \\ Y_i & p = \frac{3}{4}; \epsilon = \frac{1}{4} \\ X_i \oplus Y_i \oplus 1 & p = \frac{3}{4}; \epsilon = \frac{1}{4} \end{cases}$$

- Data complexity $\geq \epsilon^{-2}$

Linear Cryptanalysis - Data Complexity

- Data complexity $\geq \epsilon^{-2}$
- Data complexity $\leq 2^n$

Multiple Linear Cryptanalysis

- Using more than one linear approximation to reduce the data complexity

Multiple Linear Cryptanalysis

- Using more than one linear approximation to reduce the data complexity
- Using more than one linear approximation to extend the attack

The NIST Workshop

- " ...For example, the bias calculated in section 5 should be $2^{-8.34\times 2} \times 2^{-1} = 2^{17.64}$, not $2^{-8.34\times 2} \times 2 = 2^{-15.68}$. This error was propagated throughout the paper... "
  (Anonymous reviewer for the NIST)

The NIST Workshop

- " ...For example, the bias calculated in section 5 should be $2^{-8.34\times 2} \times 2^{-1} = 2^{17.64}$, not $2^{-8.34\times 2} \times 2 = 2^{-15.68}$. This error was propagated throughout the paper... "
  (Anonymous reviewer for the NIST)
- " ...The first comment, dealing with the right bias when combining two linear approximations is clearly wrong. The joint bias when combining approximations is given by the piling up lemma and is equal to (for three approximations) $e_0 \times e_1 \times e_2 \times 2^2$..." (my response to the NIST review)

The Plot Thickens

- Three days after sending this, I got an email from Doug Shors

The Plot Thickens

- Three days after sending this, I got an email from Doug Shors
- "We are preparing to post a paper to the eprint archive; one thing we've done in the paper is summarize the current state of the SIMON and SPECK cryptanalysis... " (Doug Shors, 24/05/2015)
- " ...Right now we're not seeing how it could work as claimed... " (Doug Shors, 24/05/2015)

The Plot Thickens

- Three days after sending this, I got an email from Doug Shors
- "We are preparing to post a paper to the eprint archive; one thing we've done in the paper is summarize the current state of the SIMON and SPECK cryptanalysis... " (Doug Shors, 24/05/2015)
- " ...Right now we're not seeing how it could work as claimed... " (Doug Shors, 24/05/2015)
- " ...I understand that implementing the full attack is out of reach. But is it possible to restrict the keys in some way, or to do the 22- or 23-round version of the attack, and get some useful information?" (Doug Shors, 26/05/2015)

Verifying the Attack on 20 Rounds

- Doug: " ...Combining a bunch of random biases ($2^{-n/2}$ is random), if it worked, would allow you to attack any number of rounds of any block cipher... " (Doug Shors, 26/05/2015)

Verifying the Attack on 20 Rounds

- Doug: " ...Combining a bunch of random biases ($2^{-n/2}$ is random), if it worked, would allow you to attack any number of rounds of any block cipher... " (Doug Shors, 26/05/2015)
- Tomer: " ...Combining enough linear approximations together - even if the bias for each individual one is below $2^{-n/2}$ - can improve an attack both in terms of the number of required plaintexts and/or the length of the distinguisher... " (Tomer Ashur, 26/06/2015)

Verifying the Attack on 20 Rounds

- Doug: " ...Combining a bunch of random biases ($2^{-n/2}$ is random), if it worked, would allow you to attack any number of rounds of any block cipher... " (Doug Shors, 26/05/2015)
- Tomer: " ...Combining enough linear approximations together - even if the bias for each individual one is below $2^{-n/2}$ - can improve an attack both in terms of the number of required plaintexts and/or the length of the distinguisher... " (Tomer Ashur, 26/06/2015)
- Doug: " ...Actually, I do not disagree with this statement, but you really have to consider what happens in the wrong case, which I don't think is done in the paper..." (Doug Shors, 26/06/2015)

Direct Email Exchange with the NSA

- “ ...Just as a friendly comment, I think there are some misconceptions in the paper which will be apparent to experts reading it, and so it’s probably in your interest to fix them... ” (Doug Shors, 01/06/2015)

Direct Email Exchange with the NSA

- " ...Just as a friendly comment, I think there are some misconceptions in the paper which will be apparent to experts reading it, and so it's probably in your interest to fix them... " (Doug Shors, 01/06/2015)
- "I come originally from the mathematics world, where there's a pretty high standard regarding the veracity of published results, and I'm often disappointed by the standard for crypto publications, where opinion, wishful thinking, marketing of tweaks to existing methods as fundamental breakthroughs, etc., etc., are all tolerated. I'm addressing the situation in general; not your paper in particular. Of course there is also a lot of very high-quality work out there" (Doug Shors, 26/06/2015)

Parseval's Theorem

- " ...there's the 19th-century mathematics that underlies this subject. I would urge you to review Parseval's Theorem if you have the belief that aggregating the data for all 2^{2n} approximations will lead somewhere... "

Parseval's Theorem

- " ...there's the 19th-century mathematics that underlies this subject. I would urge you to review Parseval's Theorem if you have the belief that aggregating the data for all 2^{2n} approximations will lead somewhere... "
- $\int_{-\infty}^{\infty} |x(t)|^2 \, dt = \int_{-\infty}^{\infty} |X(f)|^2 \, df$.

The Central Limit Theorem

- "We didn't do random case runs, because we think we understand that case, basically by the central limit theorem (more precisely using Berry-Esseen type results that tolerate local dependence, and bound the L^∞ distance between the wrong case distribution and the appropriate normal distribution)... "

The Central Limit Theorem

- "We didn't do random case runs, because we think we understand that case, basically by the central limit theorem (more precisely using Berry-Esseen type results that tolerate local dependence, and bound the L^∞ distance between the wrong case distribution and the appropriate normal distribution)... "
- $|F_n(x) - \Phi(x)| \leq \frac{C\rho}{\sigma^3\sqrt{n}}$

"Trust Us"

- " ...And I certainly don't have the chutzpah to think I'm so smart that I could pull something over on the likes of Shamir, Dinur, Biham, Wang, Leander, et al., that they would never discover..." (Doug Shors, 29/09/2015)

"Trust Us"

- " ...And I certainly don't have the chutzpah to think I'm so smart that I could pull something over on the likes of Shamir, Dinur, Biham, Wang, Leander, et al., that they would never discover..." (Doug Shors, 29/09/2015)
- " ...We have an Information Assurance Directorate and a Signals Intelligence Directorate. We (the SIMON and SPECK designers) work in the former. I'm sure just about every nation has something like this, and has to resolve issues that arise... " (Doug Shors, 30/09/2015)

"Trust Us"

- " ...And I certainly don't have the chutzpah to think I'm so smart that I could pull something over on the likes of Shamir, Dinur, Biham, Wang, Leander, et al., that they would never discover..." (Doug Shors, 29/09/2015)
- " ...We have an Information Assurance Directorate and a Signals Intelligence Directorate. We (the SIMON and SPECK designers) work in the former. I'm sure just about every nation has something like this, and has to resolve issues that arise... " (Doug Shors, 30/09/2015)
- " ...I know that I have really outstanding Ph.D. statisticians here that I consult when I need assistance with statistics... " (Doug Shors, 01/10/2015)

"Stop Embarrassing Yourself"

- " ...I suspect that you're sufficiently convinced that something's wrong with SIMON that you're unable to review your own work with a critical eye. If I wanted to be preachy, I'd say it's dangerous in science to "know" what the answer is before you look at the data, because you can easily end up fooling yourself... " (Doug Shors, 29/09/2015)

"Stop Embarrassing Yourself"

- " ...I suspect that you're sufficiently convinced that something's wrong with SIMON that you're unable to review your own work with a critical eye. If I wanted to be preachy, I'd say it's dangerous in science to "know" what the answer is before you look at the data, because you can easily end up fooling yourself... " (Doug Shors, 29/09/2015)
- " ...In fact I'm very careful in my work, and I've spent well over a year working to attack SIMON, so I that could be as sure as I possibly could be that it was secure. So I know what's possible. I'm not apt to accept something that I know doesn't work... " (Doug Shors, 30/09/2015)

"You're out of your League"

- " ...Is there anyone at your venerable institution that can carefully and critically review your work before you seek to publish it? I assure you that this is in your own best interest... " (Doug Shors, 29/09/2015)

"You're out of your League"

- " ...Is there anyone at your venerable institution that can carefully and critically review your work before you seek to publish it? I assure you that this is in your own best interest... " (Doug Shors, 29/09/2015)
- "I can't believe that Prof. Rijmen didn't identify the issues I've identified; I'm guessing he didn't carefully work though the paper. (I know my advisor wouldn't have...) " (Doug Shors, 30/09/2015)

"NSA Runs"

- " ...We've now generated a lot of data – 1024 trials for 30 rounds SIMON, and 1024 random case trials (for which we used the full SPECK algorithm and your approximations). In short, there's nothing there; the two distributions are not distinguishable by any test we can conceive of... " (Doug Shors, 18/10/2015)

"NSA Runs"

- " ...We've now generated a lot of data – 1024 trials for 30 rounds SIMON, and 1024 random case trials (for which we used the full SPECK algorithm and your approximations). In short, there's nothing there; the two distributions are not distinguishable by any test we can conceive of... " (Doug Shors, 18/10/2015)
- " ...Interestingly, for 18 rounds, it appears that there is likely a distinguisher. However, it's not a slam dunk... " (Doug Shors, 18/10/2015)

Moving Forward

- " ...then I would like to ask you to retract the claims in the ISO Belgium expert contribution that there are weaknesses in the Simon cipher... " (Louis Wingers, 16/10/2015)

Moving Forward

- " ...then I would like to ask you to retract the claims in the ISO Belgium expert contribution that there are weaknesses in the Simon cipher... " (Louis Wingers, 16/10/2015)
- " ...Thus, if Tomer could provide us (Doug or myself) with his results and whether you would like to retract your claim by the 21st of October, I would greatly appreciate it... " (Louis Wingers, 16/10/2015)

Moving Forward

- " ...then I would like to ask you to retract the claims in the ISO Belgium expert contribution that there are weaknesses in the Simon cipher... " (Louis Wingers, 16/10/2015)
- " ...Thus, if Tomer could provide us (Doug or myself) with his results and whether you would like to retract your claim by the 21st of October, I would greatly appreciate it... " (Louis Wingers, 16/10/2015)
- " ...then at the Study Period session in Jaipur, as Rapporteur, I will address Tomers work in detail, including his previous ePrint paper which has been largely discredited by X. Wang (who will be in attendance)... " (Louis Wingers, 16/10/2015)

Summary

- Simon has been somehow based on *Parseval's Theorem* for its design

Summary

- Simon has been somehow based on *Parseval's Theorem* for its design
- The NSA are pushing Simon and Speck really hard as standards

Summary

- Simon has been somehow based on *Parseval's Theorem* for its design
- The NSA are pushing Simon and Speck really hard as standards
- The NSA can run 2^{10} experiemnts each evaluating $2^{32} \cdot 2^{14}$ linear equations in less than one night.

Summary

- Simon has been somehow based on *Parseval's Theorem* for its design
- The NSA are pushing Simon and Speck really hard as standards
- The NSA can run 2^{10} experiemnts each evaluating $2^{32} \cdot 2^{14}$ linear equations in less than one night.
- The NSA does not understand the level of doubt academics have toward their work.

Lesson Learnd

- It seems that as far as crypto standards go, the post-snowden world looks pretty much like the pre-Snowden world