Nowości w kryptografii

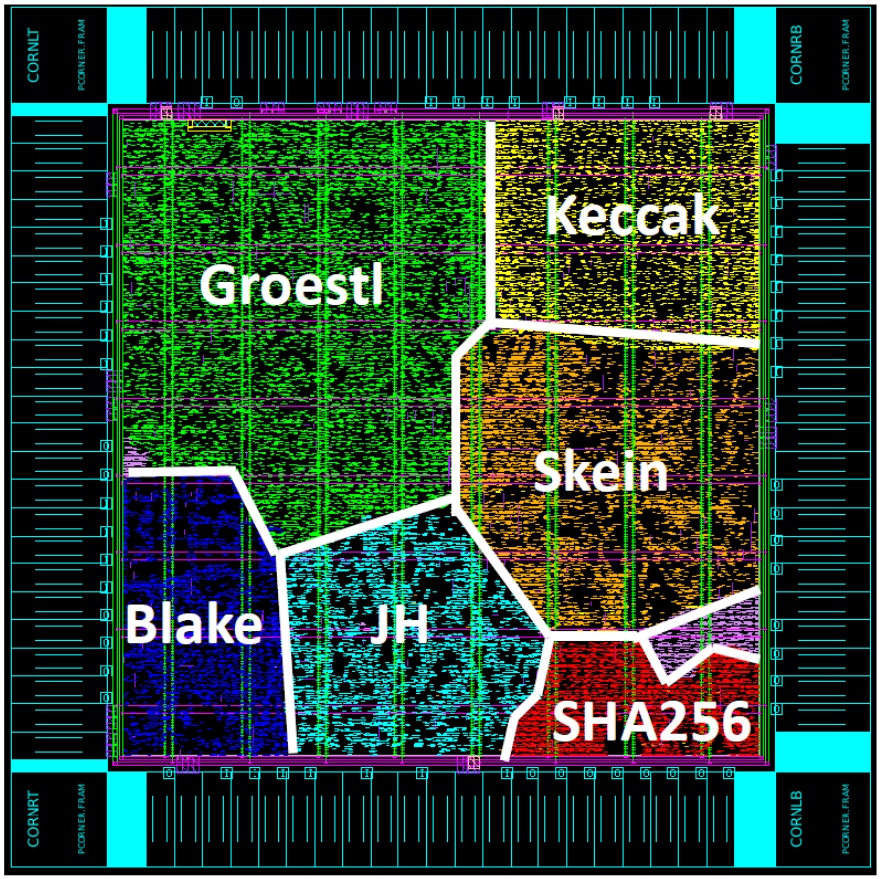
Andrzej Chmielowiec

30 maja 2012

Implementacja finalistów konkursu SHA-3 w układzie ASIC (1)

Algorytm	Przepustowość [Gbps]	Moc [mW]	Energia [mJ/Gbit]
BLAKE-256	2.13	19.77	25.00
Grostl-256	9.31	139.29	33.70
JH-256	3.05	13.01	20.63
Keccak-256	10.67	19.78	8.96
Skein512-256	3.05	51.09	26.04
SHA256	1.51	5.05	13.76

Implementacja finalistów konkursu SHA-3 w układzie ASIC (2)



Nowy FIPS 180

W marcu 2012 roku NIST opublikował nową wersję standardu FIPS 180. Dokument FIPS 180-4 wprowadza dwie funkcje skrótu:

- SHA512/224,
- SHA512/256.

Czego mężczyźni szukają w Internecie?

Czego mężczyźni szukają w Internecie?

- Zdjęć (2%),

Czego mężczyźni szukają w Internecie?

- Zdjęć (2%),
- Filmów (8%),

Czego mężczyźni szukają w Internecie?

- Zdjęć (2%),
- Filmów (8%),
- ... (89.9999999%),

Czego mężczyźni szukają w Internecie?

- Zdjęć (2%),
- Filmów (8%),
- ... (89.9999999%),
- Kluczy publicznych (0.0000001%)

Czego mężczyźni szukają w Internecie?

- Zdjęć (2%),
- Filmów (8%),
- ... (89.9999999%),
- Kluczy publicznych (0.0000001%) – Arjen Lenstra, James Hughes, Maxime Augier, Joppe Bos, Thorsten Kleinjung, Christophe Wachter.

Co można znaleźć w Internecie?

Co można znaleźć w Internecie?

- 

Co można znaleźć w Internecie?

- 
- 6.600.000 kluczy publicznych RSA

Co można zrobić ze znalezionymi modułami RSA?

Co można zrobić ze znalezionymi modułami RSA?

- 99.8% – możemy wydrukować.

Co można zrobić ze znalezionymi modułami RSA?

- 99.8% – możemy wydrukować.
- **0.2% – możemy rozłożyć na czynniki!**

Postępy w znajdowaniu logarytmu dyskretnego na krzywej eliptycznej

Za około 2.000.000 PLN można zakupić zestaw pozwalający na łamanie kluczy na 130-bitowych krzywych w ciągu jednego roku.

Postępy w znajdowaniu logarytmu dyskretnego na krzywej eliptycznej

Za około 2.000.000 PLN można zakupić zestaw pozwalający na łamanie kluczy na 130-bitowych krzywych w ciągu jednego roku.

W skład zestawu wchodzą:

Postępy w znajdowaniu logarytmu dyskretnego na krzywej eliptycznej

Za około 2.000.000 PLN można zakupić zestaw pozwalający na łamanie kluczy na 130-bitowych krzywych w ciągu jednego roku.

W skład zestawu wchodzą:

- mała Cola,

Postępy w znajdowaniu logarytmu dyskretnego na krzywej eliptycznej

Za około 2.000.000 PLN można zakupić zestaw pozwalający na łamanie kluczy na 130-bitowych krzywych w ciągu jednego roku.

W skład zestawu wchodzą:

- mała Cola,
- frytki,

Postępy w znajdowaniu logarytmu dyskretnego na krzywej eliptycznej

Za około 2.000.000 PLN można zakupić zestaw pozwalający na łamanie kluczy na 130-bitowych krzywych w ciągu jednego roku.

W skład zestawu wchodzą:

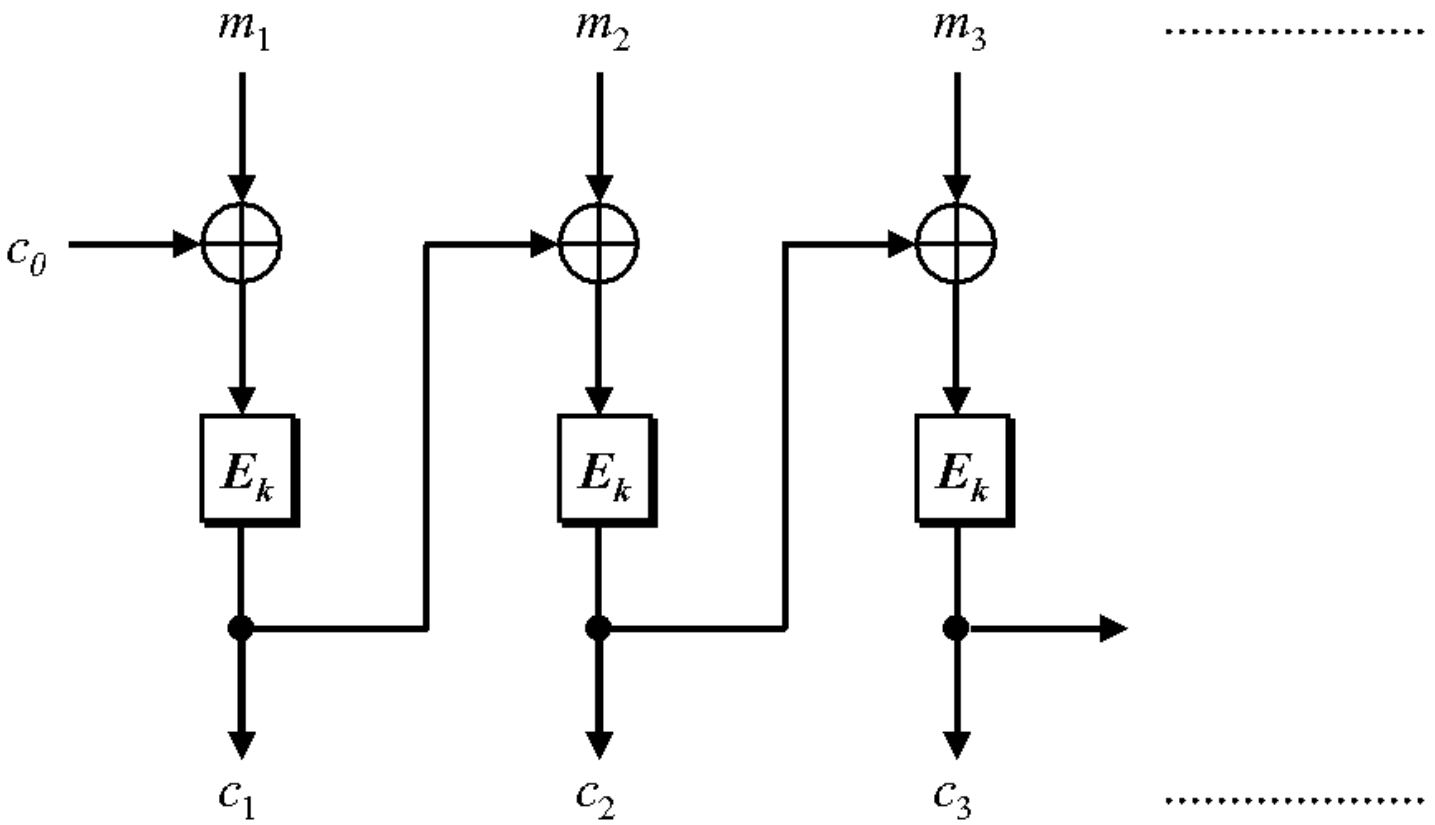
- mała Cola,
- frytki,
- 1.100 kart graficznych GTX 295.

Biclique - czyli, jak w teorii złamano AES

W 2011 roku Andrey Bogdanov, Dmitry Khovratovich i Christian Rechberger zaprezentowali pierwszy atak na szyfr AES.

Szyfr	Dane	Złożoność ataku	Pamięć
AES-128	2^{88}	$2^{126.18}$	2^{8}
AES-192	2^{80}	$2^{189.74}$	2^{8}
AES-256	2^{40}	$2^{254.42}$	2^{8}

Tryb CBC - schemat



Tryb CBC - oznaczenia

- $E_k(m)$ – funkcja szyfrująca pojedynczy blok m przy użyciu klucza k,
- $D_k(c)$ – funkcja deszyfrująca pojedynczy blok c przy użyciu klucza k,
- $m_1, ..., m_n$ – kolejne bloki tekstu jawnego,
- $c_1, ..., c_n$ – kolejne bloki szyfrogramu,
- c_0 – wektor początkowy.

Tryb CBC - szyfrowanie i deszyfrowanie

Proces szyfrowania w trybie CBC wyraża się następującą zależnością rekurencyjną:

- $c_i = E_k(m_i \oplus c_{i-1})$.

Natomiast proces deszyfrowania CBC wyraża się wzorem:

- $m_i = D_k(c_i) \oplus c_{i-1}$.

Atak na tryb CBC (1)

Rozważmy teraz scenariusz, w którym implementacja SSL/TLS wykorzystuje ostatni szyfrogram, jako wektor początkowy dla kolejnego rekordu. W takiej sytuacji każdy, kto obserwował ostatni zaszyfrowany rekord $(c_0, c_1, ..., c_\ell)$ będzie znał wektor początkowy użyty do szyfrowania kolejnego rekordu.

Załóżmy, że atakujący ma pewną hipotezę dotyczącą bloku m_j. Atakujący przypuszcza, że wartość m_j jest równa m^*. Jeśli atakujący *zmusi* użytkownika, aby na początku kolejnego rekordu zaszyfrował wiadomość:

$$m' = c_{j-1} \oplus c_\ell \oplus m^*,$$

to zweryfikuje prawdziwość swojej hipotezy.

Atak na tryb CBC (2)

$$\begin{aligned} E_k(m' \oplus c_\ell) &= E_k((c_{j-1} \oplus c_\ell \oplus m^*) \oplus c_\ell) \\ &= E_k(c_{j-1} \oplus m^*) \\ &= c'. \end{aligned}$$

Porównując szyfrogram c' z szyfrogramem $c_j = E_k(m_j \oplus c_{j-1})$ atakujący może stwierdzić, że jego hipoteza jest poprawna jeśli $c' = c_j$.

Atak BEAST

Duong i Rizzo zaproponowali rozwinięcie ataku na tryb CBC stosowany w protokole SSL/TLS. Aby to zrobić wykorzystali nowe funkcjonalności oferowane przez przeglądarki i strony WWW. Mechanizmy wymienione poniżej mogą zostać wykorzystane do przeprowadzenia bardzo praktycznego ataku na tryb CBC szyfru blokowego:

- Javascript XMLHttpRequest API,
- HTML5 WebSocket API,
- Flash URLRequest API,
- Java Applet URLConnection API,
- Silverlight WebClient API.

Ochrona przed atakiem BEAST

Aktualnie najpewniejszym sposobem na neutralizację zagrożenia jest rezygnacja po stronie serwera z obsługi protokołów SSL 3.0, TLS 1.0 i przejście na protokoły TLS 1.1 i TLS 1.2.

Kradzież ziaren do tokenów SecurID

W 2011 roku firma RSA poinformowała swoich klientów o włamaniu, którego skutkiem była między innymi kradzież ziaren (kluczy prywatnych) do tokenów SecurID. Dostęp do kluczy oraz informacja na temat algorytmu generowania kodów pozwalają symulować działanie określonego urządzenia.

Wniosek na przyszłość

**Jeśli dwie osoby mają dochować tajemnicy,
to jedna musi jej nie znać!**

Dziękuję za uwagę.