Sinople: a 128-bit symmetric block cipher

Draft - 2

Philippe Paquet

Revised, March 14, 2003

Abstract

We describe Sinople, a shared-key (symmetric) block cipher supporting 128-bit data blocks and 128-bit key size. Sinople is designed to take advantage of the 32-bit operations supported in today's computers and its original design tries to improve security against Differential and Linear attacks.

philippe@paquet.net
http://philippe.paquet.net/sinople

Content

1. Definitions

D[] is an array of 4 32-bit data words. Initially D contains the plaintext words, and at the end of the encryption process it contains the ciphertext words.

K[] is the expanded key array, consisting of 64 32-bit words.

S0[] and **S1[]** are two S-boxes, consisting of 256 32-bit words.

All the arrays below are 0-based.

$\oplus$ Bitwise exclusive-OR operation

$\boxplus$ Addition

$<<n$ Rotation to the left by *n* bits

2. Algorithm Specifications

2.1. High level structure

Sinople is an inconsistent Generalized Unbalanced Feistel Network (GUFN) [1] using 64 rounds of two different types: D (target-heavy) and C (source-heavy). The rounds are grouped in 4 blocs as show in figure 1.

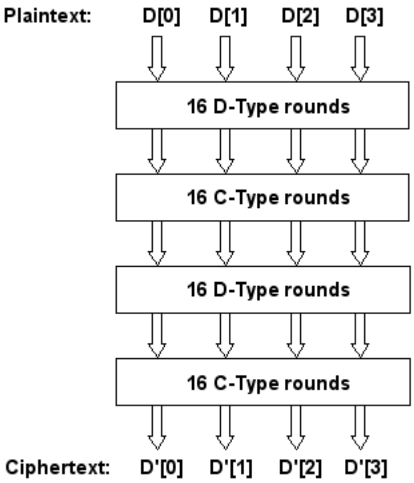

Figure 1 : High-Level structure of the cipher

2.2. D-Type round structure

The target-heavy D-Type round is designed to maximise diffusion. In D-Type rounds, **D[3]** and **K[r]** are used by a F function to alter **D[0]**, **D[1]** and **D[2]**. 8 rounds are necessary to achieves full avalanche.

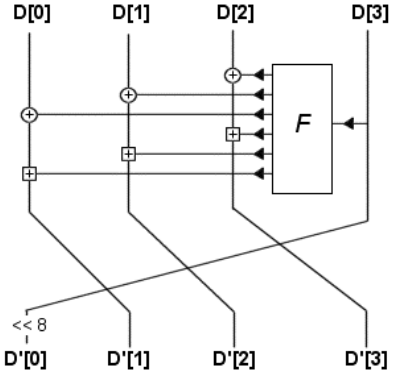

Figure 2 : D-type round structure

2.3. C-Type round structure

The source-heavy C-Type round is designed to maximise confusion. In C-Type rounds, **D[0]**, **D[1]**, **D[2]** and **K[r]** are used by an F function to alter **D[3]**. 4 rounds are necessary to achieves full avalanche.

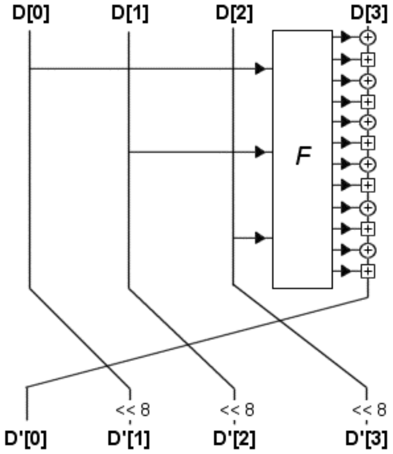

Figure 3 : C-Type round structure

2.4. D-Type round F function

In a D-Type round F function, **C** is a function which take as input **D[3]** ⊕ **K[r]**. The **C** function removes bits 0, 1, 10, 11, 20, 21, 30 and 31 to produce a 24-bit value. That 24-bit value is then sliced into 3 8-bit values that will be used as S-Boxes **S0** and **S1** inputs. Outputs of S-Boxes **S0** and **S1** are then used to alter **D[0]** , **D[1]** and **D[2]**.

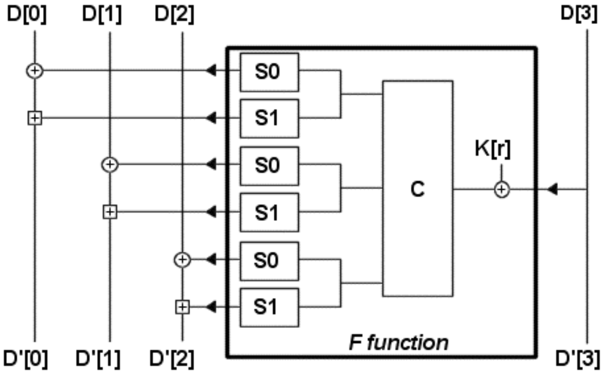

Figure 4 : D-Type round F function

2.5. C-Type round F function

In a C-Type round F function, **D[0]** ⊕ **K[r]**, **D[1]** ⊕ **K[r]** and **D[2]** ⊕ **K[r]** are sliced in 4 8-bit values that will be used as S-Boxes **S0** and **S1** inputs. Outputs of S-Boxes **S0** and **S1** are then used to alter **D[3]**.

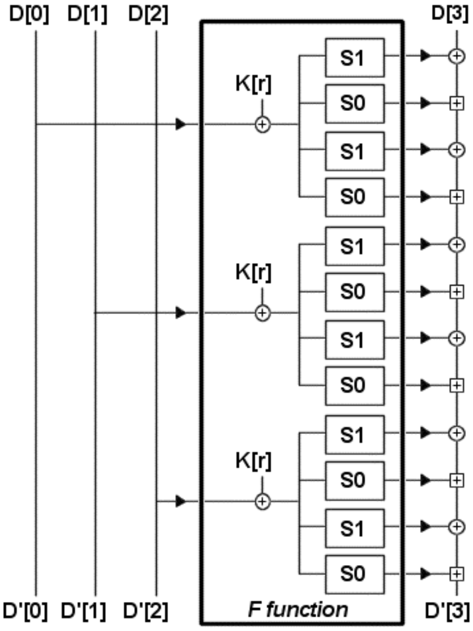

Figure 5 : C-Type round F function

2.6. Key schedule

The key schedule use blocks of 16 D-Type rounds to create sub keys. The key used is a counter starting at 0, increasing after each block of 16 D-Type rounds.

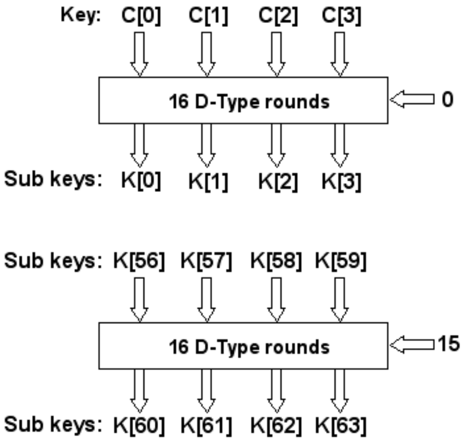
Key: C[0] C[1] C[2] C[3]
16 D-Type rounds
0
Sub keys: K[0] K[1] K[2] K[3]
Sub keys: K[56] K[57] K[58] K[59]
16 D-Type rounds
15
Sub keys: K[60] K[61] K[62] K[63]

Figure 6: Key schedule

3. Implementation details

Sinople is designed to take advantage of the 32 bit operations available on today's computers. A software implementation can achieve a very high speed. We are currently working on Intel optimised C source code [2].

As Sinople is designed to be simple, implementation in various computer languages should not be a problem.

The C++ reference implementations of Sinople has the following memory requirements:

- 256 bytes to store the expanded key
- 2048 bytes for S-Boxes

Expanding the key, encoding a block or decoding a block functions will use in the worst case less than 128 bytes of stack.

implementation on 8-bit microprocessors should not be a problem but, as Sinople is 32 bit words oriented, this will not give optimum speed.

As Sinople is only using operations commonly found on typical microprocessors, hardware implementation should not be a problem.

4. Design principles

4.1. Cipher design principles

The cipher was designed using the following principles:

- Suitable for both software and hardware implementations
- Fast
- Simple
- Low memory requirement
- High security

- D-type round has to maximize diffusion
- C-type round has to maximize confusion
- D-type rounds have to be used prior C-type rounds
- Contacts between round keys and data are made only thru S-Boxes
- Xor operations must alternate with Add operations

4.2. S-Boxes design principles

The S-Boxes are very similar to MARS S-Boxes [3]. They were designed using the following principles:

- No entries containing 0 or 0xffffffff
- Sub differences have less than two bytes equals to 0
- No equal, complement or negative pairs
- All xor differences have at least four 1 bits
- All xor and sub differences are distinct
- Parity bias must be lower than 1/32
- 1 bit bias must be lower than 1/30
- 2 bit bias must be lower than 1/30

4.3. Key schedule design principles

The key schedule was designed using the principles:

- Simple
- Share part of its procedure with encryption/decryption
- Key set up time should be shorter than encryption
- No equivalent keys
- No weak keys

In cases where large amounts of data are processed with a single key, the set-up time for key scheduling is not important. In applications in which the key is changed frequently, time for key scheduling is a factor.

5. Cryptanalysis

Sinople is designed to be simple in order to ease cryptanalysis.

As D-type and C-type rounds are designed to work in a bloc of 16, we may consider attacking a version of the cipher reduced to 32 rounds but not less.

We are currently working on cryptanalysis using Differential [4] and Linear [5] attacks.

6. References

[1] *Unbalanced Feistel Networks and Block-Cipher Design*
B. Schneier, J. Kelsey

[2] *Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor*
B. Schneier, D. Whiting

[3] *Efficient Methods for Generating MARS-like S-boxes*
L. Burnett, G. Carter, E. Dawson, W. Millan

[4] *Differential Cryptanalysis of DES-like Cryptosystems*
E. Biham, A. Shamir

[5] *Linear Cryptanalysis Method for DES Cipher*
M. Matsui

A. S-Box 0

```
0x80B26358,    0x6DD6428B,    0xEB18FBF2,    0xCF9A5DE5,
0x52338AB4,    0xCBA557D0,    0x4F3931D0,    0xEEDE690C,
0xE1F810EA,    0xCFC4FC91,    0x62203EC7,    0x7A63C227,
0xEDCC58A1,    0x17B62C48,    0x697B6E99,    0x0628DAFA,
0xF0896B35,    0xA71D2CD4,    0xC11A047A,    0x094E3E85,
0x03B2416D,    0xA2D17B44,    0x6CCDBF9E,    0x2A53FC5D,
0x8417B843,    0xA9ECD2DC,    0x17EAFE12,    0x2A2B5D54,
0xC16ED9C1,    0xA042B33F,    0x0C604729,    0xBC933AD5,
0xE6893738,    0xB7B8835D,    0x7E0EF9C9,    0xB1C65D0D,
0x260A0F19,    0x6F938178,    0x53B0FCF6,    0xE4DF5195,
0x94C6684A,    0x6F826762,    0x66233EF0,    0x11C7D942,
0x452F1A4F,    0x956737EC,    0xA000A714,    0xE9B27390,
0x03B1B4CB,    0x3BBC8AB6,    0xFD638B6C,    0x4C72922E,
0xD63CD9C5,    0x894E0A97,    0xF19F8BA2,    0xEBF0BE85,
0x5E942D64,    0x3081BB34,    0x8E4833FB,    0xF4D9B4D4,
0x2CC15A74,    0xE2C66E50,    0xC6C49908,    0xD522B89B,
0xE9B7878A,    0x42735A30,    0xAFCD72E3,    0x10D4CB7D,
0x56D6AC6F,    0x99BEF655,    0x10AEA650,    0xE31FBD7E,
0xB9E27E67,    0x3BDEAC10,    0xDCEA30C6,    0xDE6353ED,
0xD3B1B734,    0xA659954B,    0xC14CF94A,    0xA0D23FB4,
0x1E95071E,    0xE75E7E5E,    0x08228F01,    0xBCBFBD57,
0x1DAF6FDA,    0xA782AC71,    0xDB07B735,    0xD8494A42,
0x78E22620,    0x2A1C2F36,    0x36B74AC2,    0x023E19F3,
0x13F869AA,    0x073AC9B7,    0x7CEDA226,    0x4B3CCFA9,
0x73F827D8,    0xF6792CBE,    0xBE619895,    0x949CF5B0,
0xA95C2B7B,    0x2B545008,    0xAA3402A1,    0xAF404381,
0xDA1F9618,    0x9A609E84,    0xB8F66053,    0xE9D8BE6B,
0xA6837C9E,    0x8607F059,    0x8724E9FE,    0x213C444A,
0xEBFE79E0,    0x48D26E03,    0x12962A04,    0x3BE911AF,
0x7939FAE1,    0x82B16E45,    0x3C423037,    0x268F398C,
0x1DF0F347,    0x589C4782,    0xBE740D24,    0xD3380877,
0x4CC46D48,    0x32EEFA78,    0x566DEEB4,    0xE34E6086,
0xAEF1493D,    0x4EB54CD5,    0x12483A81,    0xE949C57C,
0x5F3CABC7,    0x8390D684,    0xA8CAA6C4,    0xA7661AD5,
0x98AB0A0B,    0xEBA59676,    0x1458BFA1,    0x4CB480F6,
0x328C5F4E,    0xE1C6091A,    0x80241B45,    0x37ECEDDE,
0xF8E14E67,    0xD49433F3,    0xB99F501C,    0xD7BFF7B3,
0xA6C9F2A6,    0x15564174,    0xF6BC04F8,    0x8AAD4D9F,
0x16A6791C,    0xE93979F3,    0x599A4FF2,    0xFA251592,
0x97E81968,    0x38CD3CA4,    0xC1E33A0A,    0xC25660F0,
0x1C08C7DF,    0x4D49DF2F,    0x073640B1,    0xCA02C608,
0x9A80116D,    0xF7572437,    0x4432E16C,    0x728623F3,
0x0204492F,    0x8C7800EE,    0xBF6AF2B8,    0x98DBCF56,
0x904913BE,    0x65A80C7F,    0x91A56F29,    0xD435987E,
0xB9CDC730,    0x8E5B1D54,    0x6C2634A2,    0x507245B9,
0xFE8CAFBB,    0x4E77A150,    0x2FFCC5B6,    0xB6C19A2C,
0x64F85EED,    0x7F15D598,    0x6EF09636,    0x97916533,
0xAFAA3740,    0x5DAB99F5,    0xB8AB11AA,    0xC622D751,
0x2A1557BC,    0x008708BA,    0x27031FFE,    0x83B9EF1E,
0xBF1C6A7D,    0x2CE138DD,    0x7EFA96A3,    0xB8B71C5B,
0x0AD106B9,    0x5EE74AE4,    0x609DD74C,    0x6B48ACEE,
0xF48DA75F,    0xCD69E154,    0x051E6B84,    0xC9E07370,
0x6E5D66B0,    0x7377951E,    0x994649C9,    0x6E4EE492,
0x42C3E57B,    0x2E8EF724,    0x3B3ABDA3,    0xBB2604FD,
0x7B05DB98,    0xFAD04D47,    0xD0044319,    0xE51A513B,
0xB4A3A92A,    0x3707F460,    0xDC474B4D,    0x4A6F4826,
0x252BC3C0,    0x30ACCE91,    0x4C81672C,    0x154D34A7,
0xF1702B0E,    0x4D38FAD3,    0x4A567A4F,    0x9E166CBA,
0x5C98810E,    0xC368421C,    0xF3EF9C95,    0xEA829A82,
0x5A15CC0F,    0xFA43D06B,    0x3EB40F31,    0x0DED5D04,
0x1D1688F4,    0x34F16528,    0xE227EA4E,    0x054149E9,
0x4B363315,    0xA7E57E11,    0xD023C2C3,    0x1E66227D,
0xDE2D4DF4,    0x178BD0DB,    0x8867871E,    0x3E2E2EDD,
0x73311581,    0x45319877,    0x5309D50A,    0x342F4780
```

B. S-Box 1

```
0x2883D2BF,    0x6D06C2ED,    0xBBC0E8A5,    0x9C4D9827,
0x68B6A43A,    0x076EFF68,    0xB4674931,    0x06612AEC,
0xAF0FA5CA,    0x10FC9D00,    0x895FA667,    0x2DC393AA,
0x88B11802,    0x75546CE7,    0x52FC7389,    0xF997AF66,
0x599D3371,    0x0C956A19,    0x1F886FC0,    0xA0794E40,
0x859CE835,    0xFB2298CA,    0x669E0CD9,    0x4BBB1508,
0x66E10D7C,    0xE2E4B233,    0xC2BAF581,    0x1D164DB4,
0x6D2FDE1A,    0x81937B37,    0xF816DB18,    0x18E0EA3F,
0xD5B3B309,    0x956BCD0B,    0x79E534D4,    0x7E3658E1,
0x202A7BB5,    0x3C0BE11A,    0xD8D62F12,    0x2023F019,
0xB1175428,    0xFBFE6FB0,    0xC2C60E8A,    0x354BC57B,
0xEF46361F,    0x34335297,    0x5AEE0467,    0x51722D58,
0xE326F5A1,    0x09925B51,    0xABFB8AD6,    0x4DD2FF4A,
0x6B1BBACB,    0x26983E3C,    0xA1FE9C23,    0x264ED763,
0xAC71CB8A,    0xEA8B60E2,    0x215310A2,    0x0953A2E7,
0xF5C39182,    0xD2CFF017,    0x06CCDC0E,    0xD82E0374,
0xADA63B2A,    0xA6085A77,    0x78FF0870,    0xC7702FE4,
0x102FF069,    0x81E1699A,    0xEB6A743E,    0x5E660919,
0x0C6F4A7A,    0x8D0012BD,    0x9DD5B86C,    0xC105CAFA,
0x867F0164,    0x5E4DB6DB,    0xA5313F7E,    0x63B9C6BF,
0x8EEDED7A,    0xD3AD269E,    0xB2F8FB02,    0xD2857062,
0xC2494A9E,    0x300793D3,    0xDE5255FA,    0xDE46A7EB,
0x5858F5AE,    0x4A3C8FCE,    0xED28A880,    0xAAD61D82,
0xE20FF8A9,    0x242393CA,    0xC5820824,    0xDF6414F1,
0x79BA232B,    0x0596EFE5,    0x396120D9,    0x601A4815,
0x9AC582DC,    0xBABF0118,    0xFE34192F,    0xE5593C8C,
0x54EA84BD,    0xC53547CF,    0xC0AE5C68,    0x431AE965,
0xEB115498,    0x1948EF0A,    0x1F8279E8,    0xB5F72FF2,
0xEA57DFF3,    0x1142DAF3,    0xA4B0BE26,    0x93B3A27D,
0x15FB11CD,    0xE0D6F796,    0x5EA177D7,    0x3C139A18,
0xFAC5423D,    0xDA49597D,    0xE82D89AD,    0x3A57BC6E,
0x17B0B3D1,    0x619D2BFE,    0xFD61B277,    0x574C816D,
0x46DC6F92,    0x4D7A4C0E,    0x3CC8BAFF,    0x2B858527,
0xE3BC64AF,    0x4A109ED5,    0xC1ABA37B,    0xC5D648C0,
0x3904C4D5,    0x93445AA9,    0xEC4AC530,    0x8B03C194,
0x7298F3F6,    0xF8909A4B,    0xF525EB3C,    0x2ABD869D,
0x08EDC0E9,    0xDA573EE7,    0x37666622,    0xA7E20C56,
0xC994D1AC,    0x69535C5C,    0x0A0710FE,    0x13D87044,
0x061120A6,    0x64102F2A,    0xDE22822C,    0x0802A5E5,
0x3B19469B,    0x3796A3AE,    0xDC42075A,    0x10E57116,
0x8907E58E,    0xC76CDAED,    0xE0927227,    0x5EEDA39E,
0xDB1CCA20,    0x63CD9997,    0x90EC41F5,    0xAFB34D94,
0x456A307D,    0x6F53D57B,    0xA955188A,    0x8913347D,
0xDD6BEFA9,    0xAF3D8CFE,    0x0023FA7B,    0x38D51E00,
0xEA1F855E,    0x9BD57DB5,    0x08FBC88A,    0x1CEE0768,
0xF8011EBC,    0x72501E9B,    0x4887C627,    0xF6BDA3EB,
0xD384806C,    0x121E9877,    0x70F35DA2,    0xDB855EA1,
0xC1F52A04,    0xDB22405E,    0x164F743A,    0x75EA9507,
0x4AC97165,    0x15FC4D76,    0x86733DF9,    0xA20AF90D,
0x4438DAF5,    0x03ECC5B8,    0xA6C1D612,    0x5D2806F0,
0xCF27017D,    0x66C8F507,    0x5DCFCEC4,    0xE49C07ED,
0x7731D6FE,    0xDFB0C97D,    0x9F4DEDDE,    0xB5D6E1BD,
0xE0459143,    0x33CFBD3E,    0x3FD167B3,    0xB354495D,
0x9130D7F1,    0xAB2AFBE7,    0x02BC3A4B,    0xF6D4CFDE,
0x348BFA55,    0x15BBDB33,    0x521CF5D3,    0x47370BC3,
0xADF2D9DD,    0xD0645E4B,    0xB5BE9AA2,    0x489E29CD,
0x0FBB638B,    0x8893F72D,    0x90A682AE,    0x49673A37,
0xBAC5B7B2,    0x36AAAB91,    0x1EE872C0,    0x644596FA,
0x6DF2B10E,    0xDAA4658E,    0x000D3505,    0xA834A026,
0xB0A5B244,    0x4E40F345,    0xB2EE8BF6,    0x294992F4,
0xF8D0E4F0,    0x948B9B86,    0x633AB27F,    0x8E085752,
0x1432A534,    0x916B9416,    0x5C26E12B,    0xE979E9C1,
0x813484C2,    0x4EEE8D41,    0xB47F0A94,    0xF0202F42,
0xB50F26B9,    0xF34C1F05,    0x6669BC56,    0x3041FE77
```