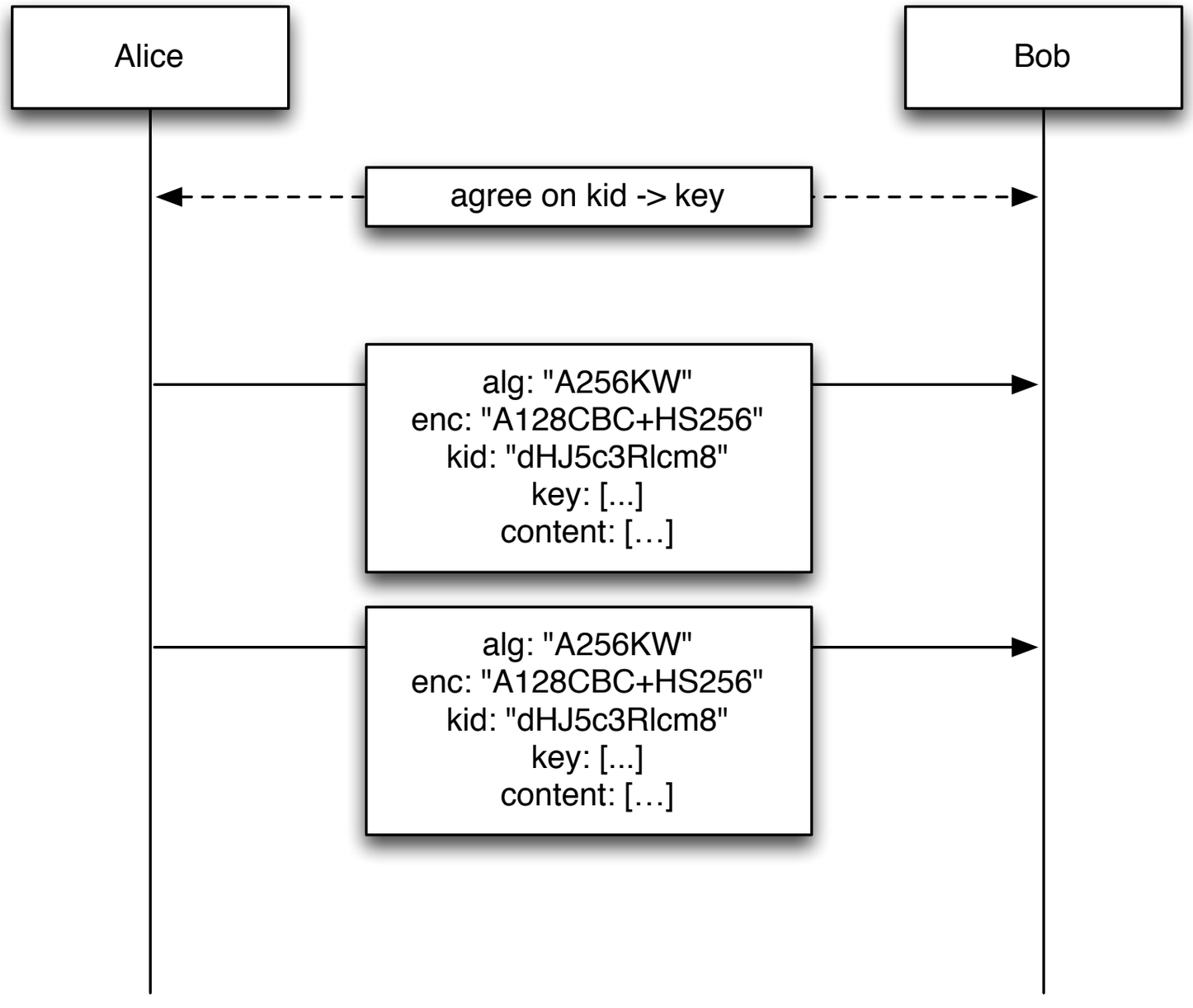
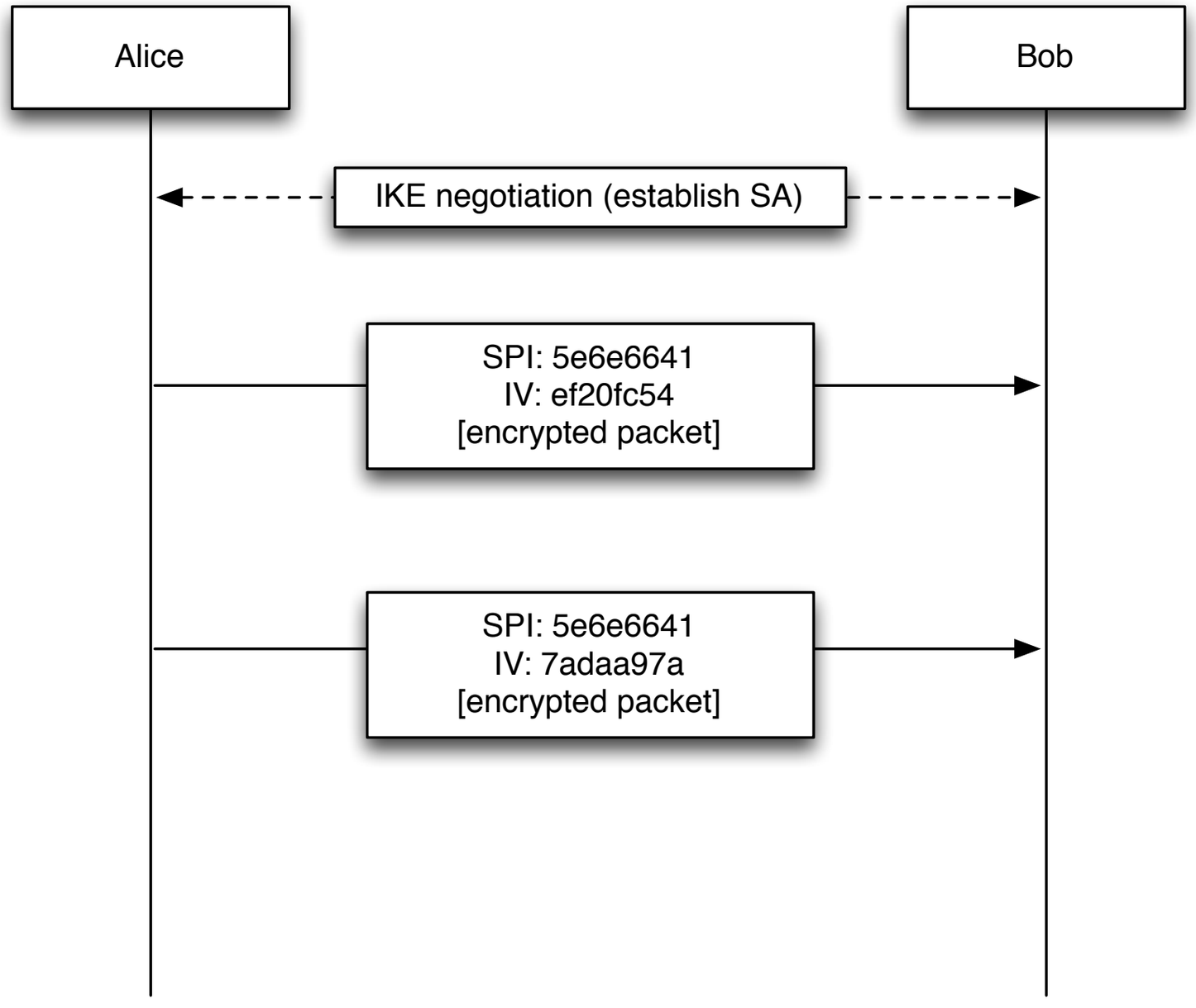
JOSE Security Parameters Index

“kid”

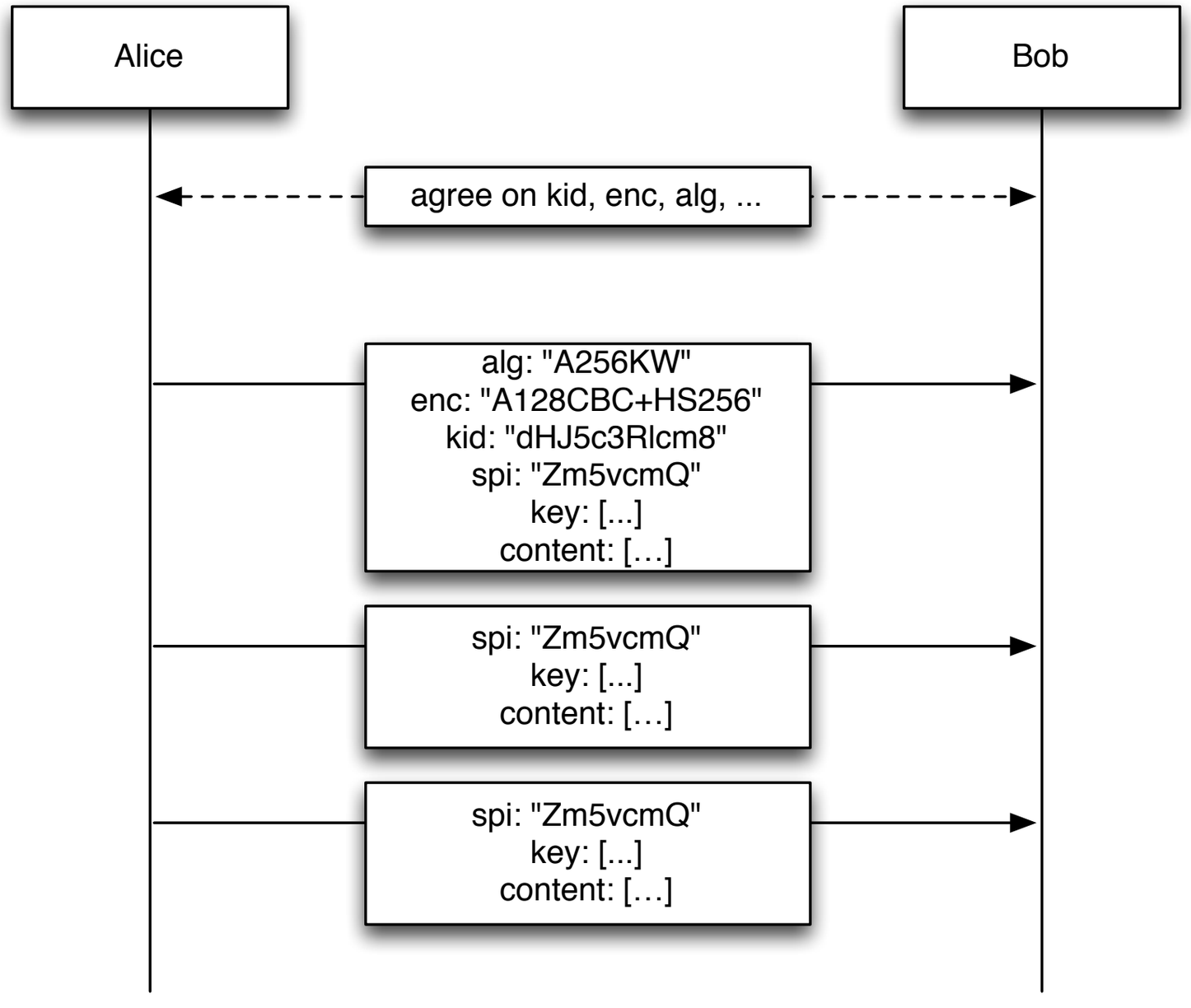

Alice
Bob
agree on kid -> key
alg: "A256KW"
enc: "A128CBC+HS256"
kid: "dHJ5c3Rlcm8"
key: [...]
content: […]
alg: "A256KW"
enc: "A128CBC+HS256"
kid: "dHJ5c3Rlcm8"
key: [...]
content: […]

IPsec


Alice
Bob
IKE negotiation (establish SA)
SPI: 5e6e6641
IV: ef20fc54
[encrypted packet]
SPI: 5e6e6641
IV: 7adaa97a
[encrypted packet]

PRE-NEGOTIATE
ALL THE PARAMETERS
quickmeme.com

“spi”


Alice
Bob
agree on kid, enc, alg, ...
alg: "A256KW"
enc: "A128CBC+HS256"
kid: "dHJ5c3Rlcm8"
spi: "Zm5vcmQ"
key: [...]
content: […]
spi: "Zm5vcmQ"
key: [...]
content: […]
spi: "Zm5vcmQ"
key: [...]
content: […]

Save on octets!

JWS

```
{"typ":"JWS","alg":"HS256",
   "kid":"dHJ5c3Rlcm8"}
```

base64url: 67B

```
{"typ":"JWS","spi":"dHJ5c3Rlcm8"}
```

base64url: 45B

33% savings!

JWE

```
{"typ":"JWE","alg":"RSA-OAEP",
"enc":"A256GCM","kid":"dHJ5c3Rlcm8"}
```

base64url: 89B

```
{"typ":"JWE","spi":"dHJ5c3Rlcm8"}
```

base64url: 45B

49% savings!